21 世纪计算机系列规划教材

网络建设与管理

主　编　张春霞　张瑞春

副主编　康文涛

電子工業出版社

Publishing House of Electronics Industry

北京・BEIJING

内 容 简 介

本书分别以Windows和Linux网络服务器操作系统为平台，从实用、够用的角度出发，讲述网络操作系统的使用和网络的组建与管理技术。全书包括10个项目：网络连接介质、安装网络服务器操作系统、企业网站的架设、部署DNS服务、部署FTP服务、部署DHCP服务、电子邮件服务器的应用、让局域网访问互联网、网络安全与监控管理、网络高效应用。

本书可作为高职高专计算机网络、计算机应用等相关专业的网络专业教材，也可供成人高等教育、技能型紧缺人才培养使用，还可作为网络管理人员及相关工程技术人员的培训教材或参考资料。

图书在版编目（CIP）数据

网络建设与管理 / 张春霞，张瑞春主编. —北京：电子工业出版社，2011.9
21 世纪计算机系列规划教材
ISBN 978-7-121-14291-8

Ⅰ. ①网… Ⅱ. ①张… ②张… Ⅲ. ①计算机网络管理－高等职业教育－教材 Ⅳ. ①TP393.07

中国版本图书馆 CIP 数据核字（2011）第 159045 号

策划编辑：柴 灿
责任编辑：郝黎明 文字编辑：裴 杰 特约编辑：李云霞
印 刷：
装 订：
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×1092 1/16 印张：9 字数：236.8 千字
印 次：2011 年 9 月第 1 次印刷
印 数：3 000 册 定价：23.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

随着计算机技术的不断发展，计算机网络已经成为人们生活中重要的组成部分。目前计算机网络已经应用到社会生活、经济建设的诸多领域。近年来，随着我国信息化进程的加快，越来越多的单位开始着手发展自己的网络建设及规模，并逐步将单位的形象及产品推向Internet，从而需要越来越多的掌握计算机网络技术的专门人才。为了适应网络时代人们对网络组建、管理方面技能的需求，本书系统地介绍网络组建与管理方面的相关知识等。

本书从岗位实际需求出发，合理安排知识结构，由浅入深、循序渐进地安排网络组建技术的相关知识。本书共分为 10 个案例项目，安排如下：项目 1，认识制作五类双绞线的工具、制作 RJ-45 接头；认识信息模块的制作工具、制作信息模块。项目 2，安装 Windows Server 2003 和 Linux 的 CentOS 网络服务器操作系统。项目 3，在 Window Server 2003 操作系统下架设企业网站，即架设 WWW 服务器及配置。项目 4，分别在 Windows Server 2003 和 Red Hat Enterprise Linux 5 平台下安装和设置 DNS 服务。项目 5，利用 Serv-U 部署 Windows 平台下的 FTP 服务；利用 Vsftp 部署 Linux 平台下的 FTP 服务。项目 6，分别部署两种平台下的 DHCP 服务。项目 7，利用 MDaemon 部署 Windows 平台下的 Mail 服务。项目 8，利用硬件设备如宽带路由器、利用软件如 ICS 或 NAT 实现局域网内计算机访问互联网。项目 9，安装、配置与管理网络安全防范软件——网络版杀毒软件；安装、配置与管理网络监控管理软件——网路岗网络监控软件。项目 10，网络的高效应用——企业即时通信网络平台的搭建。

本书的设计体现了高等职业教育的应用性、技术性和实用性特色。在编写上突出实用性，具有明显的高职高专特色，语言精练，内容丰富。在内容安排上，充分考虑了教学需求，理论与实践相结合，案例的可操作性强，深入浅出，便于学生实践技能提高。

本书由张春霞、张瑞春担任主编。康文涛担任副主编，参加编写的人员还有：宋艳、李梦、宋全有、李艳梅。在本书的编写过程中，得到了河南省教育厅职业教育教研室的大力支持，在此表示衷心感谢！

由于编者水平有限加之时间仓促，不妥与疏漏之处在所难免，敬请专家和读者批评指正，以便进一步修订完善。

目　　录

项目 1　网络连接介质——双绞线制作……1

任务一　RJ-45 接头的制作……1

任务二　信息模块的制作……5

项目 2　安装网络服务器操作系统……8

任务一　Windows Server 2003 系统……8

任务二　CentOS 操作系统……16

项目 3　企业网站的架设……20

任务一　使用 IIS 架设企业网站……20

任务二　使用 Apache 架设企业网站……37

项目 4　部署 DNS 服务……41

任务一　Windows Server 2003 部署 DNS 服务……41

任务二　Red Hat Enterprise Linux 5 部署 DNS 服务……51

任务三　BIND View 加速多出口网络互访……54

小结……62

思考与拓展……62

项目 5　部署 FTP 服务……63

任务一　利用 Serv-U 部署 Windows 平台下的 FTP 服务……63

任务二　利用 Vsftp 部署 Linux 平台下的 FTP 服务……69

项目 6　部署 DHCP 服务……74

任务一　部署 Windows 平台下的 DHCP 服务……74

任务二　部署 Linux 平台下的 DHCP 服务……89

项目 7　电子邮件服务器的应用……91

任务一　利用 MDaemon 部署 Windows 平台下的 Mail 服务……91

项目 8　让局域网访问互联网 …… 96
任务一　硬件实现访问互联网 …… 96
任务二　利用软件实现共享上网 …… 98
项目 9　网络安全与监控管理 …… 102
任务一　网络版杀毒软件安装、配置与管理 …… 102
任务二　网络岗网络监控软件安装、配置与管理 …… 116
项目 10　网络高效应用 …… 128
任务一　企业即时通信网络平台的搭建 …… 128

项目 1

网络连接介质——双绞线制作

学习目标

网络通信中，主机发出的数据必须经过介质传输到目的主机。当前局域网中主要使用的传输介质是五类双绞线。本项目通过若干任务达到以下学习目标：

- 认识双绞线、信息模块；
- 熟悉双绞线、信息模块制作工具；
- 熟练掌握双绞线、信息模块的制作过程。

内容框架

项目 1 的内容框架如图 1.1 所示。

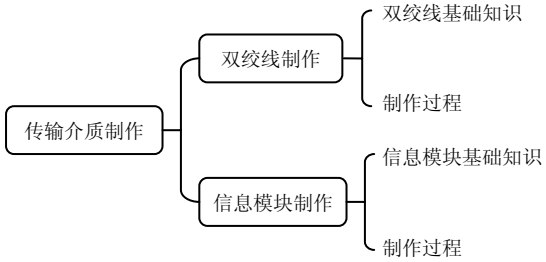

图 1.1　内容框架

任务一　RJ-45 接头的制作

1.1.1　任务目的

本任务的目的在于熟悉制作双绞线的工具以及制作过程，从而能够熟练、正确制作 RJ-45 接头。

1.1.2　任务描述

利用双绞线制作工具，制作直通和交叉双绞线。

1.1.3 相关基础知识

1．认识双绞线

双绞线是局域网组网的常用介质。双绞线是由不同颜色的 4 对 8 芯线组成的，每两条按一定规则绞织在一起，成为一个芯线对。将两根具有绝缘保护层的铜导线按一定密度互相绞缠在一起形成一个线对，可降低信号干扰的程度，一根导线在传输过程中辐射的电波会被另一根导线上发出的电波抵消。常用的双绞线是由 4 个线对按一定的密度逆时针相互绞在一起（每对密度不同），外部包裹金属层或塑料外皮。铜导线的直径为 0.4～1mm，其扭绞方向为逆时针，绞距为 3.81～14cm，相邻线对的扭绞长度差约 1.27cm。双绞线的缠绕密度和扭绞方向以及绝缘材料直接影响它的特性阻抗、衰减和近端串扰等技术指标。

双绞线可以用来传输模拟声音信息（如电话业务），但同样适用于数字信号传输，主要用于短距离的信息传输。采用双绞线的局域网的带宽取决于所用导线的质量、长度及传输技术。

双绞线按其外部包缠外皮材料的不同，可分为屏蔽双绞线和非屏蔽双绞线，如图 1.2、图 1.3 所示。

图 1.2　非屏蔽双绞线（UTP）

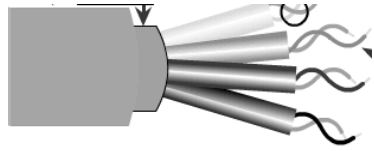

图 1.3　屏蔽双绞线（STP）

非屏蔽双绞线（UTP）是由多根线在外包裹一层塑料护套构成的，没有屏蔽层、较细小，具有安装简便、成本低等优点；屏蔽双绞线（STP）是在护套内增加了金属层，价格较高，安装相对困难，它必须配有支持屏蔽功能的特殊连接器和相应的安装技术，但它具有较高的传输速率，100M 内可达到 155Mb/s。

综合布线时常用双绞线分 100Ω和 150Ω两种。100Ω双绞线又分为 3 类、4 类、5 类及 6 类/E 级几种。150Ω双较线目前只有 5 类一种。每一种电缆又由不同数量的双绞线对组成。常用的双绞线有 4 个线对，这些线对被标示了不同的颜色，如表 1-1 所示。

表 1-1　导线色彩编码

线　　对	1	2	3	4
色 彩 码	蓝白、蓝	橙白、橙	绿白、绿	棕白、棕

目前采用以太网标准组建局域网，大多使用双绞线和交换机构成星形网络拓扑，在以太网的标准中双绞线的有效距离为 100m。

2．RJ-45 水晶头

如使双绞线能够与网卡、Hub、交换机等设备相连，还需要 RJ-45 接头，俗称水晶头，如图 1.3 所示。在制作接头时必须符合国际标准，美国电子工业协会 EIA 和美国电信工业协会 TIA 制定的双绞线制作标准有 T568A 和 T568B，对线序排列有明确规定。两种标准在制作双绞线时的线序如表 1-2 所示，RJ-45 接头及引针号如图 1.4、图 1.5 所示（注意 RJ-45 接头

的方向）。

表 1-2　线序标准

引 针 号	1	2	3	4	5	6	7	8
T568A 标准	绿白	绿	橙白	蓝	蓝白	橙	棕白	棕
T568B 标准	橙白	橙	绿白	蓝	蓝白	绿	棕白	棕

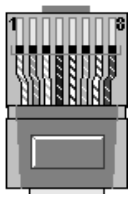

图 1.4　RJ-45 接头

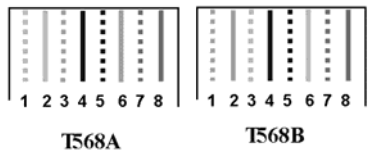

图 1.5　T568A 和 T568B 引针号

3．双绞线网线的制作工具

在双绞线网线制作中，最简单的方法只需一把网钳即可，如图 1.6 所示。它具有剪线、剥线和压线 3 种用途。剥线也可以使用专用的剥线工具，常见的 3 种剥线钳如图 1.7 所示。

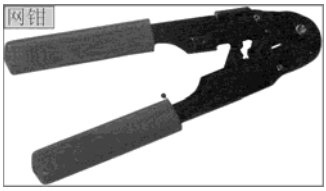

图 1.6　网钳

图 1.7　3 种剥线钳

4．测试工具

双绞线制作完成后，需要确保双绞线的连通性，这时需要借助测试工具。常用的测试工具有万用表、电缆扫描仪（Cable Scanner）、电缆测试仪（Cable Tester）3 种。

（1）万用表。万用表是测试双绞线是否正常的基本工具，但是使用起来不太方便。它只能测量单条芯线（一条芯线的两端）是否连通，因此，勉强可以得知这端接头的第几只脚是对应到另一端的第几只脚，但不能测出信号衰减情况。

（2）电缆扫描仪。电缆扫描仪除了可检测导线的连通状况外，还可以得知信号衰减率，并直接以图形方式显示双绞线两端接脚对应状况等。因其价格昂贵，通常只有专业布线厂商才会使用。

（3）电缆测试仪。电缆测试仪是比较便宜的专用网络测试器，通常测试仪一组有两个：一个为信号发射器；另一个为信号接收器，双方各有 8 只 LED 灯及至少一个 RJ-45 插槽。

1.1.4　实现参考

公司要组建一局域网，交换机、路由器、PC 等都已购置，现需要把各种设备连接起来。

虽然局域网中使用的连线有双绞线、光纤、同轴电缆等多种，但主要使用的还是双绞线。同种设备相连需要交叉双绞线，异种设备相连需要直通双绞线，该如何制作这两类双绞线呢？

【实验一】 制作直通双绞线

为了保持制作的网线有最佳的兼容性，通常采用通用的 EIA/TIA568B 标准来制作。

【实验步骤】

（1）剥线。取双绞线一头，用网钳剪线刀口将双绞线端头剪齐，再将双绞线端头伸入剥线刀口，使线头触及前挡板，然后适度握紧网钳同时慢慢旋转双绞线，让刀口划开双绞线的保护胶皮，取出端头，剥下保护胶皮。

注意：握网钳力度不能过大，否则会剪断芯线；剥线的长度为 13～15mm，不宜太长或太短。

（2）理线。双绞线由 8 根有色导线两两绞合而成，将其整理平行，从左到右按橙白、橙、绿白、蓝、蓝白、绿、棕白、棕色平行排列，整理完毕后用剪线刀口将前端修齐；顺时针方向排列。

（3）插线。将 8 根线并拢后用网钳剪齐，并留下约 12mm 的长度。一只手捏住水晶头，将水晶头有弹片一侧向下，另一只手捏平双绞线，稍稍用力将排好的线平行插入水晶头内的线槽中，8 根导线顶端应插入线槽顶端。将并拢的双绞线插入 RJ-45 接头时，注意“橙白”线要对着 RJ-45 的第一脚。

（4）压线。确认所有导线都到位后，将水晶头放入网钳夹槽中，用力捏网钳，压紧线头即可。

注意：压过的 RJ-45 接头的 8 只金属脚一定要比未压过的低，这样才能够顺利地嵌入芯线中。优质的网钳必须在接脚完全压入后才能松开握柄，取出 RJ-45 接头，否则接头会卡在压接槽中取不出来。

【实验二】 制作交叉双绞线

【实验步骤】

（1）剥线。方法同制作直通双绞线。

（2）理线。方法同制作直通双绞线。

（3）插线。方法同制作直通双绞线。

（4）压线。方法同制作直通双绞线。

（5）取双绞线另一头按照上述方法完成剥线、理线、插线、压线各步骤。

注意：在理线步骤中，双绞线 8 根有色导线从左到右的顺序是按绿白、绿、橙白、蓝、蓝白、橙、棕白、棕色顺序平行排列的，其他步骤相同。

【实验三】 测试

用电缆测试仪测试双绞线，测试时将双绞线的两端分别插入信号发射器和信号接收器，打开电源。如果测试仪上 8 只指示灯都依次为绿色闪过，证明网线制作成功。如果出现任何一只灯为红色或黄色，都证明存在断路或者接触不良的现象，此时最好先对两端水晶头再用网线钳压一次再测，如果故障依旧，再检查一下两端芯线的排列顺序是否一样，如果不一样，便剪掉一端重新按另一端芯线排列顺序制作水晶头。如果芯线顺序一样，但测试仪上仍显示

红色灯或黄色灯，则表明其中肯定存在对应芯线接触不良。此时可以先剪掉一端重做一个水晶头，如果故障消失，则不必重做另一端水晶头，否则还需把原来的另一端水晶头也剪掉重做，直到测试通过为止。

【总结】

做线时应该注意以下两点：第一，无论是左手或者右手拿线，一定要按线序号为 1 的线对齐水晶头引脚为 1 的引脚；第二，剥线时长度不宜太长，特别是剪齐后不要留太长，否则无法把做的线压紧。

思考：

1．思考直通双绞线的使用场合。
2．思考交叉双绞线的使用场合。
3．考察双绞线中每根芯线的用途。
4．尝试利用万用表测试直通双绞线和交叉双绞线。
5．考察双绞线的布线标准。
6．思考利用双绞线组网的主要网络拓扑结构，并写出所需要的主要网络部件。

任务二　信息模块的制作

1.2.1　任务目的

本任务的目的在于熟悉信息模块的制作工具及制作过程，从而能够熟练正确地制作信息模块。

1.2.2　任务描述

利用专用信息模块制作工具，制作信息模块。

1.2.3　相关基础知识

1．信息插座

信息插座一般是安装在墙面上，主要是为了保持整个布线的美观，方便移动和连接工作站，主要有桌面型和地面型两种，如图 1.8 所示。信息模块安装在信息插座内。

图 1.8　信息插座

2．信息模块

信息模块的作用类似于电源插座，一般是通过卡位固定到信息插座中。安装在信息模块上的网线其另一端连接到交换机、Hub 或其他网络设备上。图 1.9 所示为一些信息模块的外形。

信息模块各引脚的对应顺序，在信息模块的各线槽中都有相应的颜色标注。制作时只需要选择相应的端接方式（是 T568B 标准还是 T568A 标准），可以按模块上的颜色标志把相应的芯线插入相应的线槽中，不必记颜色顺序。由于信息模块的两端主要用来连接异种网络设备，所以网线的线序采用直连线式（即两端采用同一接线规范标准）。

信息模块目前有两种：一种是传统的需要手工打线的，打线时需要专门的打线工具，制作起来较麻烦；另一种是新型的，无须手工打线，无须任何模块打线工具，只需把相应的双绞芯线插入相应位置，然后用手轻轻一压即可，使用起来非常方便、快捷。在此主要介绍打线的模块制作方法。

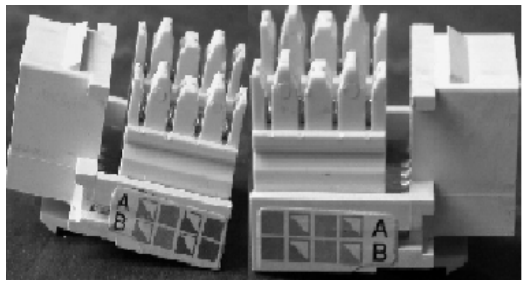

图 1.9　信息模块的外形

3．打线工具

信息模块制作，需要剥线工具和打线工具。剥线工具主要可以完成剪线、剥线两种用途。制作信息模块使用的剥线工具与制作双绞线的剥线工具一样，在此不再赘述。打线工具主要用来把已卡入卡线槽中的芯线打到卡线槽的底部，以使芯线与卡线槽接触良好、稳固。几种常用的打线工具如图 1.10 所示。

图 1.10　常用的打线工具

1.2.4　实现参考

【实验一】 制作需要打线的信息模块

【实验步骤】

（1）剥线。用剥线工具在离双绞线一端 4～5cm 长度，把双绞线的外包皮剥去。

（2）理线。把剥开的 4 对双绞线芯线分开（但为了便于浅色线的区分，在卡相应芯线前

最好不要拆开各芯线线对），按照信息模块上所指示的芯线颜色线序，两手平拉上一小段对应的芯线，稍稍用力将导线一一置入相应的线槽内。

（3）压线。全部芯线都嵌入好后，用打线工具把已卡入卡线槽中的芯线打到卡线槽的底部，以使芯线与卡线槽接触良好、稳固。操作时对准相应芯线，往下压，当卡到底时会有“咔”的声响。注意打线工具的卡线缺口旋转位置。

（4）整理。全部打完线后再对照模块上的色标检查一次，对于打错位置的芯线用打线工具的线钩勾出，重新打线。对于还未打到底的芯线，可用打线工具的压线刀口重新压一次。最后剪掉模块外多余的线。打线全部完工后，用网钳的剪线刀口或者其他剪线工具，剪除在模块卡线槽两侧多余的芯线（一般仅留 0.5cm 左右的长度）。

（5）测试。用测试仪进行测试（也可以用万用表或其他方式测试），有问题的线可以再用打线工具处理，直至全通为止。若没有问题，就可以将信息模块卡入信息插座内并固定好。

【总结】

主要讲述了信息模块的制作过程，包括剥线、理线、压线、整理、测试 5 个过程。通过以上 5 步，基本可以实现信息模块的正确制作。

项目 2

安装网络服务器操作系统

学习目标

作为服务器操作系统，高性能、高可靠性和高安全性是其必备要素，尤其是日趋复杂的企业应用和 Internet 应用，对其提出了更高的要求。微软的新一代网络操作系统 Windows Server 2003 和 Linux 操作系统 CentOS 适应了这一要求，是搭建企业级服务器的理想平台。本任务主要介绍了 Windows Server 2003 和 CentOS 服务器操作系统的安装及其作为网络操作系统的应用。

内容框架

项目 2 的内容框架如图 2.1 所示。

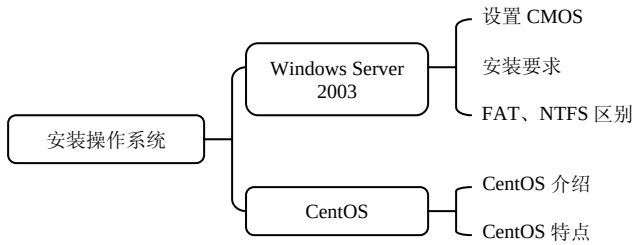

图 2.1　内容框架

任务一　Windows Server 2003 系统

2.1.1　任务目的

本任务的目的在于掌握 Windows Server 2003 的安装过程，能够正确地对安装过程中的一些选项施行正确设置。

2.1.2　任务描述

在一台充当服务器的 PC 上，安装 Windows Server 2003 网络操作系统。

2.1.3　相关基础知识

1．设置 CMOS 实现光盘引导

CMOS（本意是指互补金属氧化物半导体，一种大规模应用于集成电路芯片制造的原料）是微机主板上的一块可读写的 RAM 芯片，用来保存当前系统的硬件配置和用户对某些参数的设定值。CMOS 可由主板的电池供电，即使系统掉电，信息也不会丢失。

BIOS 即微机的基本输入/输出系统（Basic Input-Output System），是集成在主板上的一个 ROM 芯片，其中保存有微机系统最重要的基本输入/输出程序、系统信息设置、开机上电自检程序和系统启动自举程序。在主板上可以看到 BIOS ROM 芯片。一块主板性能优越与否，在一定程度上取决于板上的 BIOS 管理功能是否先进。在 BIOS 中主要有 BIOS 中断例程；BIOS 系统设置程序；POST 上电自检；BIOS 系统启动自举程序。

其中，BIOS 系统启动自举程序是指在完成 POST 自检后，ROM BIOS 将按照系统 CMOS 设置中的启动顺序搜寻软、硬盘驱动器及 CDROM、网络服务器等有效的启动驱动器，读入操作系统引导记录，然后将系统控制权交给引导记录，由引导记录完成系统的启动。

2．Windows Server 2003 对系统的要求

Windows Server 2003 对系统的要求如表 2-1 所示。

表 2-1　Windows Server 2003 对系统的要求

要　求	Standard Edition	Enterprise Edition	Data Center Edition	Web Edition
最低 CPU 速度	133MHz	• 基于 x86 的计算机：133MHz； • 基于 Itanium 的计算机：733MHz*	• 基于 x86 的计算机：400MHz； • 基于 Itanium 的计算机：733MHz*	133MHz
推荐 CPU 速度	550MHz	733MHz	733MHz	550MHz
最小 RAM	128MB	128MB	512MB	128MB
推荐最小 RAM	256MB	256MB	1GB	256MB
最大 RAM	4GB	• 基于 x86 的计算机：32GB； • 基于 Itanium 的计算机：64GB*	• 基于 x86 的计算机：64GB； • 基于 Itanium 的计算机：128GB*	2GB
多处理器支持	1 或 2 个	多达 8 个	• 要求最少 8 个 • 最多 32 个	1 或 2 个
安装所需磁盘空间	1.5GB	• 基于 x86 的计算机：1.5GB； • 基于 Itanium 的计算机：2.0GB*	• 基于 x86 的计算机：1.5GB； • 基于 Itanium 的计算机：2.0GB*	1.5GB

3．FAT 与 NTFS 文件系统及其区别

（1）FAT 文件系统

通常 PC 使用的文件系统是 FAT16。如基于 MS-DOS，Windows 95 等系统都采用了 FAT16 文件系统。在 Windows 9X 下，FAT16 支持的分区最大为 2GB。计算机将信息保存在硬盘上称为“簇”的区域内。使用的簇越小，保存信息的效率就越高。在 FAT16 的情况下，分区越大，簇就相应的要增大，存储效率就越低，势必造成存储空间的浪费。并且随着计算机硬件

和应用的不断提高，FAT16 文件系统已不能很好地适应系统的要求。在这种情况下，推出了增强的文件系统 FAT32。

（2）NTFS 文件系统

NTFS 文件系统是一个基于安全性的文件系统，是 Windows NT 所采用的独特的文件系统结构，它是建立在保护文件和目录数据基础上，同时照顾节省存储资源、减少磁盘占用量的一种先进的文件系统。使用非常广泛的 Windows NT 4.0 采用的就是 NTFS 4.0 文件系统，相信它所带来的强大的系统安全性一定给广大用户留下了深刻的印象。Windows 2000，Windows 2003 采用了更新版本的 NTFS 文件系统 NTFS 5.0，它的推出使得用户不但可以像 Windows 9X 那样方便、快捷地操作和管理计算机，同时也可享受到 NTFS 所带来的系统安全性。

2.1.4 实现参考

某公司组建了自己的局域网，可以实现内部的互相访问，也可以访问 Internet 网。现在想构建某种网络服务器，提供网络服务。因为 Windows 2003 网络操作系统可以提供高性能、高可靠性和高安全性，所以选择在服务器上安装 Windows 2003 网络操作系统，作为某种网络服务的平台。如何在服务器上安装 Windows 2003 网络操作系统？

【实验一】 安装 Windows 2003 系统

安装前要做好如下准备工作：

① 准备好支持自引导的 Windows Server 2003 安装光盘。② 用纸张记录安装序列号。③ 如果想在安装过程中格式化 C 盘、D 盘（建议安装过程中格式化 C 盘），请备份 C 盘、D 盘有用的数据。如果是新硬盘就无须备份了。

【实验步骤】

（1）当计算机加电启动时，首先运行 BIOS 驱动，即看到的第一个界面就是 BIOS 驱动界面。这时按“Del”键直到进入主板 CMOS 设置界面。在 CMOS 设置界面中选择“Advanced BIOS Features”项，将其中的“First Boot Device”项设置为 CD-ROM 值，即计算机在引导时首先从 CD-ROM（光驱）引导系统。

（2）启动系统并将 Windows Server 2003 安装光盘放入光驱，计算机通过 BIOS 自检后自动进入蓝色背景的 Windows Server 2003 安装前自检界面，该自检过程主要对计算机硬件、磁盘分区情况、已安装的系统等进行检测，需要等 2～3min。自检通过后，系统将进入 Windows Server 2003 安装界面，如图 2.2 所示。

（3）在 Windows Server 2003 安装界面中有 3 个选项：

① 现在安装 Windows 2003，请按“Enter”键。② 用“恢复控制台”修复 Windows 2003 的安装，请按“R”键。③ 停止安装 Windows 2003 并退出安装程序，请按“F3”键。

现在选第①项，即按“Enter”键来全新安装 Windows 2003，系统将进入 Windows Server 2003 许可协议界面，如图 2.3 所示。

（4）按“F8”键接受微软协议，进入磁盘分区界面，如图 2.4 所示。

在磁盘分区界面可以创建或删除磁盘分区，如创建磁盘分区按“C”键，进入创建分区界面，如图 2.5 所示。

在创建分区界面可以设置分区的大小，本例中磁盘大小为 3096MB。确认要创建该分区按“Enter”键，分区创建成功后，将返回到磁盘分区界面，如图 2.6 所示。通过该方法可以

创建多个分区。通常创建的第一个分区为 C 区。磁盘分区完之后，选择 Windows 2003 的安装分区并按“Enter”键，进入文件系统选择界面，如图 2.7 所示。为了保证服务器的安全，通常采用 NTFS 格式化磁盘（如果是新创建的磁盘分区，通常不采用快速格式化）。选择格式化方式后，按“Enter”键，进入磁盘格式化界面，格式化完毕之后自动进入系统安装文件复制界面，复制完毕系统自动重新启动，无须人工干预。

图 2.2　Windows Server 2003 安装界面

图 2.3　Windows Server 2003 许可协议界面

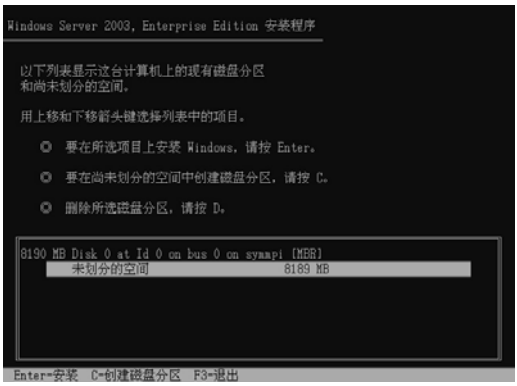

图 2.4　磁盘分区界面

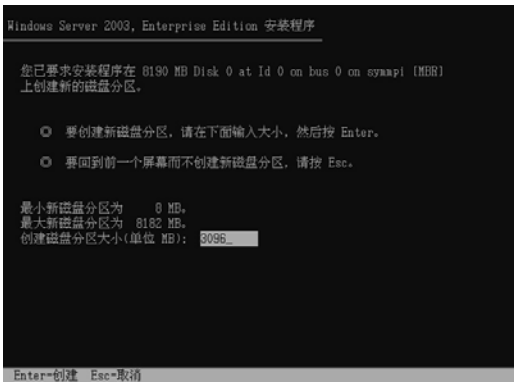

图 2.5　创建分区界面

图 2.6　返回磁盘分区界面

图 2.7　文件系统选择界面

（5）重新启动后，系统会继续安装，如图 2.8 所示。在检测设备和安装设备其间会黑屏

（闪动）两次，这是正常现象。在检测和安装设备之后，会弹出区域和语言选项界面，如图 2.9 所示。

图 2.8　Windows 安装界面

图 2.9　区域和语言选项界面

在区域和语言选项界面可以选择服务器所在位置的时区和系统的默认字体。一般采用默认值。单击“下一步”按钮，安装程序进入自定义软件界面，如图 2.10 所示。

自定义软件界面要求管理员输入管理员的姓名及服务器（或管理员）所属单位的名称，以后在本服务器上安装软件时，安装程序将自动您现在提供的个人信息。单击“下一步”按钮，进入产品密钥界面，如图 2.11 所示，在该界面中需要输入微软授权的密钥（即产品序列号）。

图 2.10　自定义软件界面

图 2.11　产品密钥界面

（6）单击“下一步”按钮，进入授权模式界面，如图 2.12 所示。授权模式界面要求选择授权模式。如果您选择“每设备或每用户”模式，那么访问运行 Windows Server 2003 家族产品的服务器的每台设备或每个用户都必须具备单独的“客户端访问许可证”。通过一个 CAL，特定设备或用户可以连接到任意数量的运行 Windows Server 2003 家族产品的服务器。拥有多台运行 Windows Server 2003 家族产品的服务器的公司大多采用这种授权方法。

“每服务器”许可证是指每个与此服务器同时连接时都需要一个单独的 CAL。换句话说，此服务器在任何时间都可以支持固定数量的连接。例如，如果选择具有 5 个许可证的“每服务器”客户端授权模式，那么该服务器一次可以具有 5 个并发连接（如果每一个客户端需要一个连接，那么一次可允许 5 个客户端）。使用连接的客户端不需要任何其他许可证。

每服务器授权模式常常是只有一台服务器的小公司的首选。这种授权模式对于 Internet 或远程访问服务器也很有用：客户端计算机可能没有被授权为 Windows Server 2003 家族产品的网络客户端。可以指定并发服务器连接的最大数量并拒绝任何额外的登录请求。

如果不能确定使用哪种模式，那么请选择“每服务器”，因为您可以一次性地从“每服务器”模式更改为“每设备或每用户”模式，而且无须任何代价。

（7）综上分析，选择“每服务器”授权模式，单击“下一步”按钮，进入计算机名称和管理员密码界面，如图 2.13 所示。计算机名称即网络上的服务器名；输入的管理员密码在登录系统时使用，一定要牢记该密码，否则安装完毕后将无法登录系统。单击“下一步”按钮，进入日期和时间设置界面，如图 2.14 所示。

图 2.12　授权模式界面

图 2.13　计算机名称和管理员密码界面

通过日期和时间设置界面，可以设置系统的日期、时间及时期。设置完毕，单击“下一步”按钮，进入完成安装界面，在完成安装界面安装程序会自动完成各项配置并删除不必要的临时文件，大约需要十几分钟。完成安装之后，系统会自动重新启动，表示整个安装过程完成。

安装完成后，重启系统便可进入 Windows Server 2003 登录界面，如图 2.15 所示。按“Ctrl+Alt+Delete”组合键弹出登录窗口，在登录窗口中输入正确的用户名称和密码即可进入系统。

图 2.14　日期和时间设置界面

图 2.15　Windows Server 2003 登录界面

【实验二】 配置 Windows Server 2003 客户机 TCP/IP 协议

【实验步骤】

如果计算机在安装 Windows Server 2003 时连接在网络中，Windows Server 2003 自动检测网卡并安装相应的协议，默认协议为 TCP/IP 协议。

配置 TCP/IP 协议，应以管理员身份登录 Windows Server 2003，右键单击“本地连接”图标，在弹出菜单上选择属性，弹出“本地连接状态”窗口，在该窗口单击“属性”按钮，弹出“本地连接 属性”对话框，如图 2.16 所示。然后选择“Internet 协议（TCP/IP）”项，单击“属性”按钮，弹出“Internet 协议（TCP/IP）属性”对话框，如图 2.17 所示。

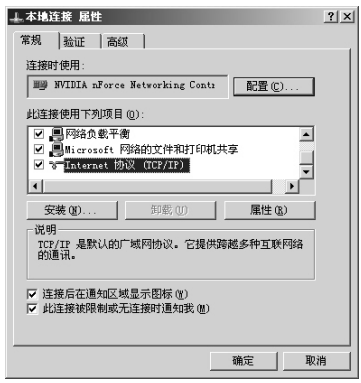

图 2.16 “本地连接 属性”对话框

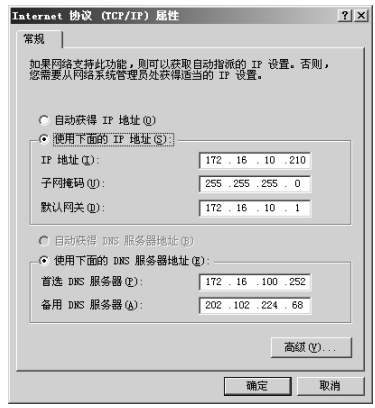

图 2.17 “Internet 协议（TCP/IP）属性”对话框

如果在局域网络中已经配置了 DHCP 服务，并且由 DHCP 服务器指定其他网络相关设置（如网关、DNS、Wins），选择“自动获得 IP 地址”和“自动获得 DNS 服务器地址”。否则在该窗口指定 IP 地址、网关、DNS。设置完毕之后，一定要单击“确定”按钮。

用户可以在安装系统时指定计算机名称及其所属的域，也可以在安装后指定计算机名称及其所属的域。

以管理员身份登录 Windows Server 2003，右键单击“我的电脑”图标，在弹出菜单上选择“属性”，弹出“系统属性”对话框，选择“计算机名”选项卡，如图 2.18 所示。单击“更改”按钮，弹出“计算机名称更改”对话框，如图 2.19 所示。在该对话框中可以指定计算机名称及其所属的域后，单击“确定”按钮完成设置。

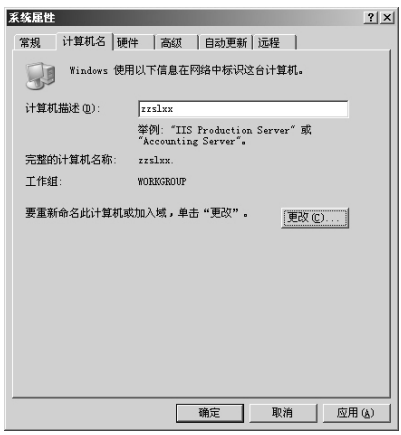

图 2.18 “系统属性”对话框

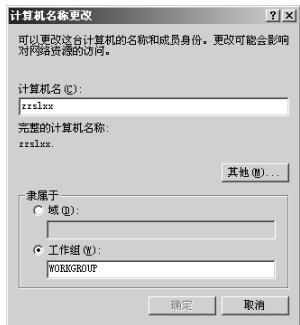

图 2.19 “计算机名称更改”对话框

【实验三】 测试客户机/服务器网络的 TCP/IP 协议

【实验步骤】

TCP/IP 协议配置之后，可以使用 Ipconfig、Winipcfg、ping、Nslookup 命令测试客户机/服务器网络的 TCP/IP 协议。

利用 Ipconfig 和 Winipcfg 命令查看网络中与 TCP/IP 协议有关的配置。在发现和解决 TCP/IP 网络问题时，首先需要检查计算机上的 TCP/IP 配置，如 IP 地址、网关、子网掩码等。这两个工具在 Windows 9X 中都能使用，功能基本相同，只是 Ipconfig 是以 DOS 的字符形式显示的，在 Windows 9X/2000/XP/2003 中都可以使用；而 Winipcfg 则用图形界面显示，只能在 Windows 9X 中使用。

使用带/all 参数的 Ipconfig 命令时，将给出所有接口的详细配置报告，可以了解当前计算机使用的网卡类型、主机的 IP 地址、子网掩码、DNS 地址和默认网关地址，甚至包括任何已配置的串行端口和网络适配器的物理地址，如图 2.20 所示。如果 IP 地址是从 DHCP 服务器租用的，Ipconfig 将显示 DHCP 服务器的 IP 地址和租用地址预计失效的日期。

图 2.20　Ipconfig 命令窗口

使用 ping 可以测试计算机名称和计算机的 IP 地址，验证与远程计算机的连接，通过将 Icmp 回显数据包发送到计算机并侦听回复数据包来验证与一台或多台远程计算机的连接状况，该命令只有在安装了 TCP/IP 协议后才可以使用。

其格式为：pingIP 地址|计算机名|域名

当使用 ping 命令后，可以通过接收对方的应答信息来判断源主机与目的主机之间的链路状况。若链路良好，则会接收到如图 2.21 所示的应答信息；若链路不通，则会接收到如图 2.22 所示的应答信息。

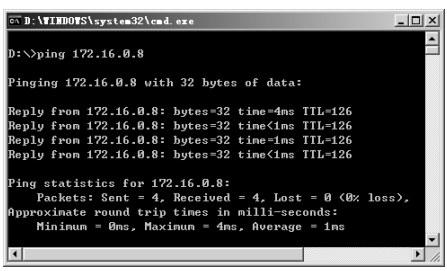

图 2.21　ping 命令链路良好应答信息图

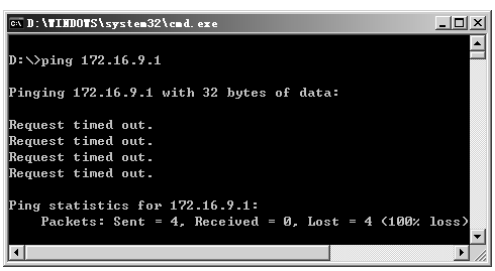

图 2.22　ping 命令链路不通应答信息图

凡是应用 TCP/IP 协议的局域网或广域网络，当客户端之间无法正常进行访问，或者网络工作出现各种不稳定的情况时，建议大家使用 ping 命令测试网络的通信是否正常。

【总结】

安装 Windows 2003 操作系统比较简单，易于掌握。在选择授权模式时，一定要结合自己网络实际情况选择“每客户模式”或“每服务器模式”，如果暂时不清楚，可选择“每服务器模式”。

思考：

1．为什么要将计算机的启动顺序设置为“CD-ROM”优先？

2．初始磁盘分区是在 Windows 2003 安装之前、之后还是之中进行的？

3．为什么要将“服务器许可证”中的“每服务器，同时连接数”的连接数进行适当的设置？

任务二　CentOS 操作系统

2.2.1　任务目的

本任务的目的在于掌握 CentOS 的安装过程，能够正确对安装过程中的一些选项施行正确设置。

2.2.2　任务描述

在一台充当服务器的 PC 上，用 CentOS 的镜像文件安装上操作系统。

2.2.3　相关基础知识

1．CentOS 简介

CentOS 是 Community ENTerprise Operating System 的简称，有很多人称它为社区企业操作系统，无论怎么叫它，它都是 Linux 的一个发行版本。

CentOS 并不是全新的 Linux 发行版，倘若一说到 RedHat 这个大名，大家似乎都听过，在 RedHat 家族中有企业版的产品，它是 Red Hat Enterprise Linux（以下称为 RHEL），CentOS 正是这个 RHEL 的克隆版本，RHEL 是很多企业采用的 Linux 发行版本，需要向 RedHat 付费才可以使用，并能得到付过费用的服务和技术支持和版本升级。这个 CentOS 可以像 REHL 一样的构筑 Linux 系统环境，但不需要向 RedHat 付任何的费用，同样也得不到任何有偿技术支持和升级服务。

在构成 RHEL 的大多数软件包中，都是基于 GPL 协议发布的，也就是常说的开元软件，正因为这样，Red Hat 公司也遵循这个协议，将构成 RHEL 的软件包公开发布，只要遵循 GPL 协议，任何人都可以在原有的软件构成的基础上再开发。CentOS 就是这样在 RHEL 发布的基础上将 RHEL 的构成克隆再现的一个 Linux 发行版本。RHEL 的克隆版本不止 CentOS 一个，

还有 White Box Enterprise Linux 和 TAO Linux 和 Scientific Linux。

虽然说是 RHEL 的克隆，但并不是一模一样的，所说的克隆是具有 100%的互换性（真的吗？）。但这并不能保障对应 RHEL 的软件在 CentOS 上面也能够 100%的正常工作，并且安全漏洞的修正和软件包的升级对应 RHEL 的有偿服务和技术支持来说，数日、数星期、数个月的延迟情况也有。

2．CentOS 的特点

（1）能把 CentOS 理解为 Red Hat AS 系列！它完全是对 Red Hat AS 进行改进后发布的！各种操作、使用和 RedHat 没有差别！

（2）CentOS 完全免费，不存在 RedHat AS4 需要序列号的问题。

（3）CentOS 独有的 yum 命令支持在线升级，能即时更新系统，不像 RedHat 那样需要花钱购买支持服务！

（4）CentOS 修正了许多 RedHat AS 的 BUG！

（5）CentOS 版本说明：CentOS 3.1 等同于 RedHat AS3 Update1，CentOS 3.4 等同于 RedHat AS3 Update4，CentOS 4.0 等同于 RedHat AS4，CentOS 5.0 等同于 RedHat AS5。

2.2.4　实现参考

【实验一】 CentOS 5.3 的安装

【实验步骤】

（1）将 CentOS 镜像文件转换成的 CD 或 VCD 光盘放入光驱中。光驱引导，出现选择安装模式画面，如图 2.23 所示。在图中的 Boot:后面，可以直接按回车键，进入图形化模式。如果在后面输入：Linux TEXT 回车，就开始文本安装模式。这里直接按回车键，采用图形安装模式。

（2）回车后出现检测界面，检测光盘镜像文件是否完整。一般不会有问题，可以直接选择跳过，进入图 2.24。图 2.24 是 CentOS 正式开始安装界面，直接单击“Next”按钮。

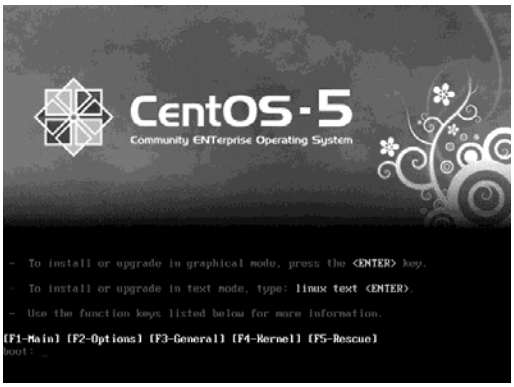

图 2.23　安装模式选择

图 2.24　正式开始安装

（3）进入语言选择界面如图 2.25 所示，选择简体中文，单击“Next”按钮，进入键盘格式选择界面如图 2.26 所示，选择“美国英语式”键盘。

图 2.25　语言选择界面

图 2.26　键盘格式选择界面

（4）从键盘选择界面进入分区界面如图 2.27 所示。在图中的分区方式框体里面，有如下 3 种选择：① 在选定的驱动器上删除所有分区并创建默认分区结构。就是所谓的“全自动分区”，不需要做什么，系统自动帮你分。② 在选定驱动器上删除 Linux 分区并创建默认的分区结构。这个项目，只有在你硬盘里面有 Linux 格式分区的时候才用到。③ 手动创建分区。这个需要自己创建分区了。

（5）进入网络设置界面如图 2.28 所示。在图 2.28 中可以设置 IP 地址、网关、主/从 DNS 等。

图 2.27　分区界面

图 2.28　网络设置界面

（6）网络设置界面设置完成后，单击“下一步”按钮，进入时区设置。只能选择上海，单击“下一步”按钮，进入系统管理员设置密码界面，如图 2.29 所示。单击“下一步”按钮，进入如图 2.30 所示界面。

（7）安装应用程序界面如图 2.30 所示。在此界面选择“现在定制”选项，进入如图 2.31 所示界面。

（8）在图 2.31 中选择具体安装的各种服务。选择后单击“下一步”按钮。

（9）选择了需要安装的软件以后就进入安装过程，中途系统会提示换盘。安装完成后重新启动进入配置界面如图 2.32 所示。单击“下一步”按钮，可以依次配置防火墙、SELinux、日期和时间、创建用户、声卡等。设置完成以后，安装完成，重新启动，进入登录界面，如图 2.33 所示。

图 2.29　管理员密码设置界面

图 2.30　安装应用程序界面

图 2.31　软件选择安装界面

图 2.32　配置界面

防火墙：配置防火墙时可以选择信任的服务和端口。SELinux：安全增强式 Linux（SELinux, Security-Enhanced Linux）是一种强制存取控制（Mandatory Access Control）的实现。它的做法是以最小权限原则（Principle of Least Privilege）为基础，在 Linux 核心中使用 Linux 安全模式（Linux Security Modules）。日期和时间：设置日期和时间。创建用户：设置一个自己的个人账号。因为 CentOS 系统第一次登录时，不允许用 rooot 账号登录的，因此这里必须要有一个其他的账号来登录系统。声卡：进行声卡测试。附加光盘：CentOS 官方提供了一套“附加光盘组件。

图 2.33　登录界面

（10）登录界面如图 2.33 所示，输入设置的个人用户名和密码登录进入系统。

【总结】

安装 CentOS 前需要把下载的镜像文件刻录成 VCD 或 DVD 格式的光盘。安装过程中可以根据实际情况进行网络参数的设置，在创建新用户窗口时尽量创建一个普通账户。

项目 3

企业网站的架设

学习目标

在网络时代，一个公司想快速、高效、省钱地宣传自己，最好的办法就是架设自己公司的网站，让大众从网络上了解公司。本项目就是讲解如何在 Windows Server 2003 操作系统下架设企业网站，即架设 WWW 服务器（或称为 Web 服务器）及配置。

内容框架

项目 3 的内容框架如图 3.1 所示。

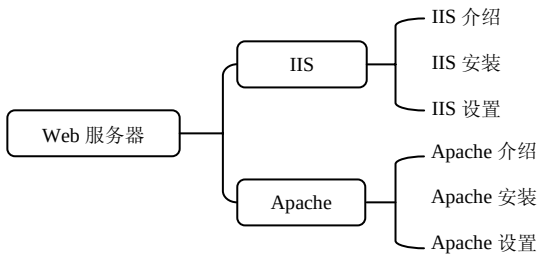

图 3.1　内容框架

任务一　使用 IIS 架设企业网站

3.1.1　任务目的

本任务的目的在于掌握 IIS 的安装及设置，从而对利用 Windows Server 2003 自带的网页发布系统有一定的认识。

3.1.2　任务描述

在一台安装了 Windows Server 2003 的计算机上，把 IIS 安装上去，并设置、调试成功，使其可以发布网页。

3.1.3　相关基础知识

IIS 是 Internet Information Server 的缩写。Internet 信息服务器是用户创建信息服务器的最重要的组件，它是微软公司主推的服务器，其最新的版本是 Windows 2003 中包含的 IIS 6.0。IIS 可以与 Windows NT Server 完全集成在一起，因而用户能够利用 Windows NT Server 和 NTFS（NT File System，NT 的文件系统）内置的安全特性，建立强大、灵活且安全的 Internet 和 Intranet 站点。

IIS 支持 HTTP（Hyper Text Transfer Protocol，超文本传输协议），FTP（File Transfer Protocol，文件传输协议）及 SMTP 协议，通过使用 CGI 和 ISAPI，IIS 可以实现高度的扩展。通过 IIS，开发人员就可以开发出新一代动态的、富有魅力的 Web 站点。IIS 不需要开发人员学习新的脚本语言或者编译应用程序，因为其完全支持 VBScript、JScript 开发软件及 Java，也支持 CGI 和 WinCGI，以及 ISAPI 扩展和过滤器。

IIS 6.0 是 Windows Server 2003 的一个组件，可以使 Windows Server 2003 成为一个 Internet 信息的发布平台，为系统管理员创建和管理 Internet 信息服务器提供各种管理功能和操作方法。但系统管理员在利用 IIS 6.0 创建 Internet 信息服务器之前，必须确认在安装系统时已经安装了 IIS，否则还需要另外安装 IIS 6.0。

在 Windows Server 2003 中，IIS 6.0 与系统进行了很好的集成，提供了许多一级组件，其中一些与相关的服务和工具绑定在一起，管理员可以根据需要的服务来选择所需的组件。IIS 的核心组件包括 Internet 服务管理器（安装基于 HTML 版本的 IIS 管理界面）、FrontPage 服务器扩展（以方便使用 FrontPage 和 Visual InterDev 来创建和管理站点和发布内容）、Internet 信息服务管理单元（可以将 IIS 的管理界面安装到 MMC 中）、Web 服务（可以使 HTTP 协议响应 TCP/IP 网络上的 Web 客户端请求）、文件传输协议服务（为建立用于上传或下载的 FTP 站点提供支持）、NNTP Service（提供简单网络新闻服务）、SMTP Service（提供简单邮件传输功能）和公用文件（提供所需要的 IIS 程序文件）等。另外，IIS 还支持其他一些功能强大的组件，如 XML、ASP、ISAPI（Internet 服务器应用程序编程接口）、IDC（Internet 数据连接器）、JVM（服务器端的 Java 虚拟机）、JSP、JavaScript、VBScript 和 CGI（公共网关接口）等，这些组件直接影响到服务器所提供的内容和功能。

IIS 6.0 与 Windows Server 2003 中的其他组件不同，它是一个 Internet 信息服务平台。IIS 6.0 提供的众多服务都是用来完成它的核心功能的，而且这些服务都可以应用到 Internet 上的信息服务中，其中最常用、最重要的服务是 Web 服务和 FTP 服务，它们也是在安装 IIS 6.0 时默认安装的服务。安装了 IIS 6.0 的服务器就成为了 Internet 信息服务器，它对内可以服务本地局域网络，对外可以服务 Internet。

3.1.4　实现参考

某公司欲申请有几个公网 IP 地址，其中一个 IP 地址为 202.102.99.99，子网掩码为 255.255.255.0。现要用这个地址作为 Web 服务器的访问地址，如何架设该 Web 服务器？

【实验一】 安装 IIS

【实验步骤】

为了更好地防止用户的恶意攻击，保护系统安全，在默认情况下，Windows Server 2003

没有自动安装 IIS 6.0，系统管理员需要单独安装 IIS 6.0，以创建 Internet 信息服务器。管理员可以通过使用控制面板中的“添加或删除程序”向导来安装此组件，具体操作步骤如下：

（1）依次选择“开始”→“管理工具”→“配置您的服务器向导”命令，在打开的向导页中依次单击“下一步”按钮。配置向导自动检测所有网络连接的设置情况，若没有发现问题则进入“服务器角色”向导页，如图 3.2 所示。

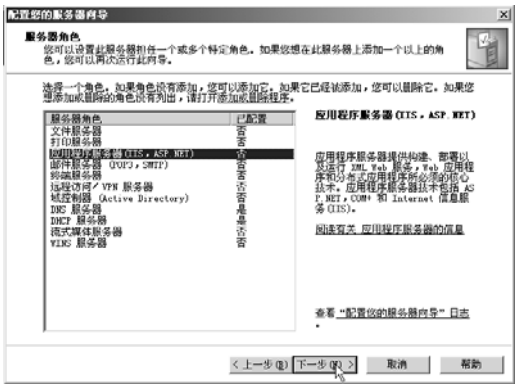

图 3.2　应用程序服务器对话框

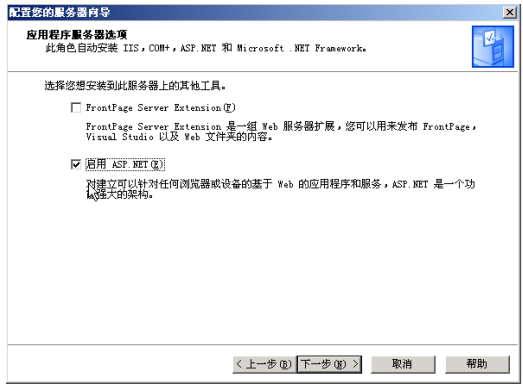

图 3.3　应用程序服务器选项

小提示：如果是第一次使用配置向导，则还会出现一个“配置选项”向导页，单击“自定义配置”单选框即可。

（2）在“服务器角色”列表中单击“应用程序服务器（IIS,ASP.NET）”选项，并单击“下一步”按钮，进入图 3.3 所示界面。

（3）在“应用程序服务器选项”对话框中，选择“启用 ASP.NET”复选项，并单击“下一步”按钮，如图 3.3 所示。

（4）向导开始安装应用程序服务器时，因为 IIS 6.0 是 Windows Server 2003 的一个组件，在后续安装时系统也会提示要求插入系统盘，插入光盘后单击“确定”按钮，如图 3.4 所示。

（5）在完成 IIS 6.0 的安装之后，向导进入最后的完成安装对话框，单击“确定”按钮即可完成创建。

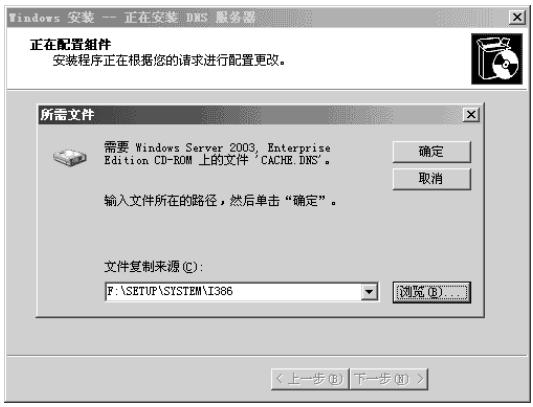

图 3.4　指定系统安装盘或安装源文件

【实验二】 创建 Web 网站

【实验步骤】

在安装 IIS 6.0 时，系统会自动创建一个名称为“默认网站”的 Web 网站，管理员通过它可以实现 Web 内容的快速发布。但是，如果管理员要发布的内容比较多，而且有不同的主题，应在服务器上创建不同的 Web 网站，再分别进行信息服务，使得一个站点具有一个主题。

（1）单击“开始”菜单，选择“管理工具”→“Internet 服务管理器”命令，打开“Internet 信息服务（IIS）管理器”窗口，在控制台目录树中展开服务器节点，如图 3.5 所示。

（2）在控制台窗口的“网站”节点上单击右键，从弹出的快捷菜单中选择“新建”→“网站”命令，打开“网站创建向导”对话框，如图 3.6 所示。

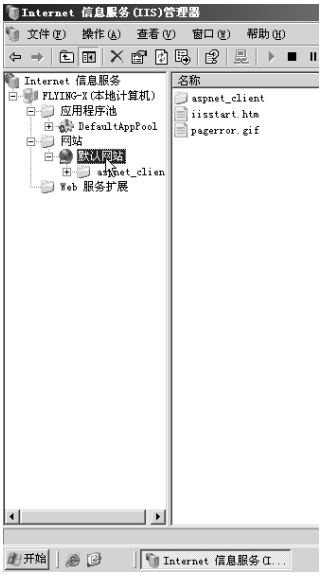

图 3.5 “Internet 信息服务（IIS）管理器”窗口

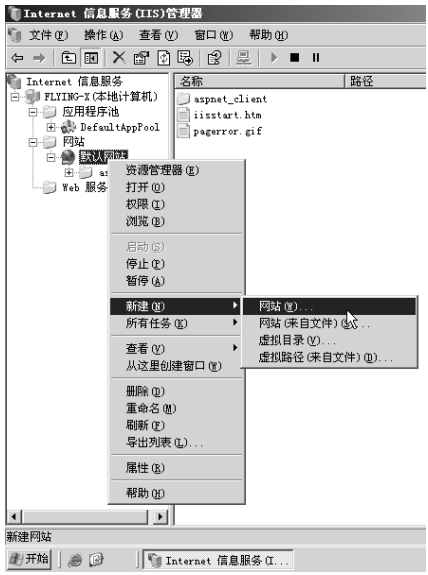

图 3.6 “网站创建向导”对话框

（3）单击“下一步”按钮，打开“网站描述”对话框，在“描述”文本框中输入站点说明即站点名称，以用于帮助管理员识别站点，如图 3.7 所示。

（4）单击“下一步”按钮，打开“IP 地址和端口设置”对话框，在“网站 IP 地址”下拉列表框中选择或直接输入 IP 地址；在“网站 TCP 端口”文本框中输入 TCP 端口值，其默认值为 80；如果有主机头，可在“此网站的主机头”文本框中输入主机头（网站对应的域名地址），系统默认为“无”，如图 3.8 所示。

图 3.7 “网站描述”对话框

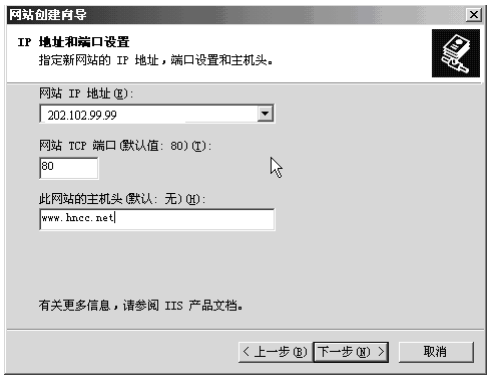

图 3.8　网站 IP 地址和端口设置

（5）单击“下一步”按钮，打开“网站主目录”对话框，在“路径”文本框中输入主目录的路径，或单击“浏览”按钮选择路径。如果允许访问者匿名访问此站点，则选中“允许匿名访问网站”复选框，如图 3.9 所示。

图 3.9　网站主目录

（6）单击“下一步”按钮，打开“网站访问权限”对话框，在“允许下列权限”选项区域中设置主目录的访问权限，为了站点安全，在“网站访问权限”对话框中不要轻易选中“读取”和“写入”复选框，这样网站访问者将能够查看和修改站点文件的内容，从而对站点构成威胁，如图 3.10 所示。

（7）单击“下一步”按钮，打开“完成网站创建向导”对话框后，再单击“完成”按钮即可完成站点的创建，如图 3.11 所示。

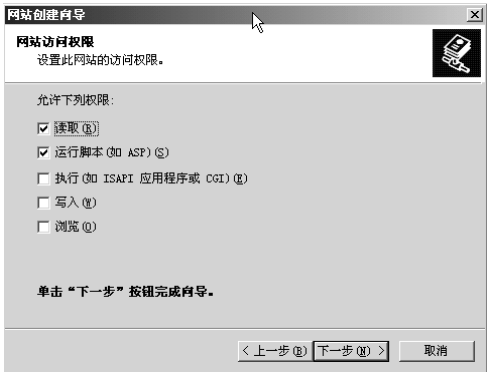

图 3.10　网站访问权限图

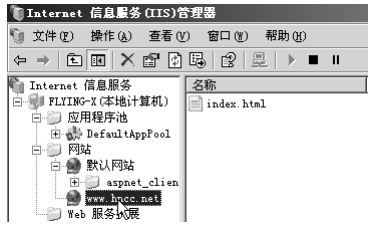

图 3.11　完成网站创建

【实验三】 Web 站点管理

【实验步骤】

在创建了网站之后，还需要对网站的属性进行相应的设置，才能更好地发挥其功能。

（1）设置网站主目录

主目录是站点的中心，通常它包含带有欢迎内容的主页或索引文件，并且也包含站点到其他主要 Web 页面的所有链接。每个 Web 网站都必须有一个主目录。主目录映射为站点的域名或服务器名。在创建新的网站时，管理员也需要选择站点的主目录。而在确定主目录之后，管理员只需将要发布的内容复制到该目录下即可。

设置主目录的具体操作步骤如下：单击“开始”菜单，选择“管理工具”→“Internet 信

息服务管理器”命令，打开“Internet 信息服务”窗口。在控制台目录树中展开服务器节点，然后在要设置主目录的网站列表选项上单击鼠标右键，在弹出的快捷菜单中选择“属性”命令，打开其属性对话框后，选择“主目录”选项卡。

在“主目录”选项卡中，管理员通过 3 个单选按钮可以选择主目录内容的来源位置。如果选中“此计算机上的目录”单选按钮，管理员可以将本地计算机上的目录作为该站点的主目录；如果选中“另一台计算机上的共享”单选按钮，管理员可以从本地局域网络中的其他计算机上查找目录并作为主目录；如果选中“重定向到 URL”单选按钮，管理员也可将主目录的目录内容重定向到 Internet 上的某个 Web 网站。

在该选项卡中，将目录本地路径、权限及应用程序设置好之后，单击“确定”按钮即可完成主目录的设置，如图 3.12 所示。

（2）添加虚拟目录

虚拟目录是网站中除主目录之外的其他发布目录。要从主目录以外的其他目录中进行内容发布，就必须创建虚拟目录。虚拟目录不包含在主目录中，但在显示给客户浏览器时就像位于主目录中一样。虚拟目录有一个“别名”，以供 Web 浏览器用于访问此目录。别名通常比目录的路径名短，这样便于访问者输入；而且使用别名更安全，因为访问者不知道文件是否真的存在于服务器上，所以便无法使用这些信息来修改文件；使用别名还可以更方便地移动站点中的目录。若要更改目录的 URL，只需更改别名与目录实际位置的映射即可。

对于简单的网站一般不需要添加虚拟目录，可以将所有文件放置在站点的主目录中，但是，如果站点比较复杂或者需要为网站的不同部分指定不同的 URL 时，可按需要创建虚拟目录。

添加虚拟目录的具体步骤如下：

① 打开“Internet 信息服务”窗口，在控制台目录树中展开服务器节点，在要创建虚拟目录的站点或者其下级目录上单击鼠标右键，在弹出的快捷菜单中选择“新建”→“虚拟目录”命令，打开“虚拟目录创建向导”对话框，如图 3.13 所示。

图 3.12 “主目录”选项卡

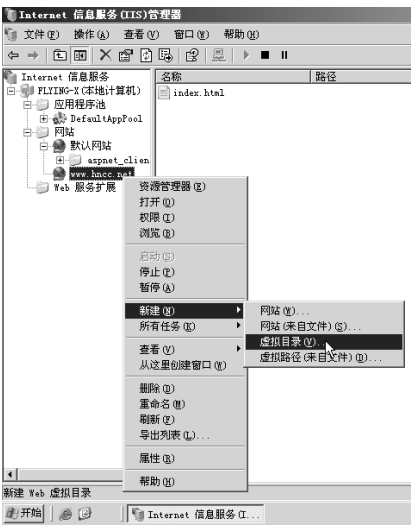

图 3.13　创建虚拟目录

② 然后单击“下一步”按钮，打开“虚拟目录别名”对话框，在“别名”文本框中输入用于获得此网站的虚拟目录访问权限的别名，如图 3.14 所示。

③ 输入别名后，单击“下一步”按钮，打开“网站内容目录”对话框，在“路径”文本框中输入或者选择虚拟目录的来源路径，如图 3.15 所示。

图 3.14　虚拟目录别名

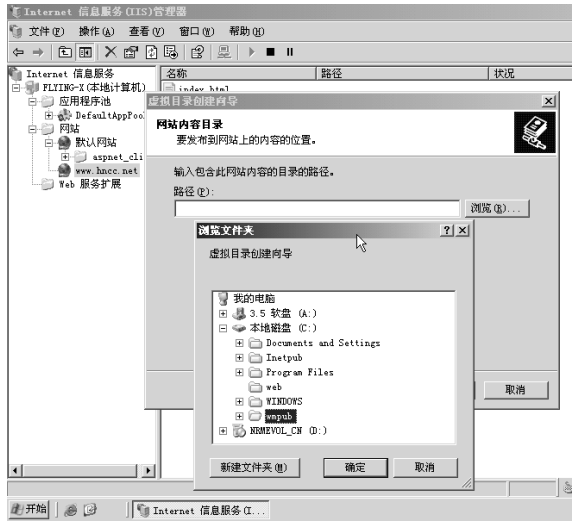

图 3.15　网站内容目录

④ 单击“下一步”按钮，打开“网站访问权限”对话框，在“允许下列权限”选项区域中为此目录设置访问权限，如图 3.16 所示。

⑤ 访问权限设置完成后，单击“下一步”按钮，打开“虚拟目录创建完成”对话框，单击“完成”按钮，虚拟目录即可创建完成。在控制台窗口中，虚拟目录和实际目录（不带别名的目录）都显示在 Internet 服务管理器中，如图 3.17 所示。

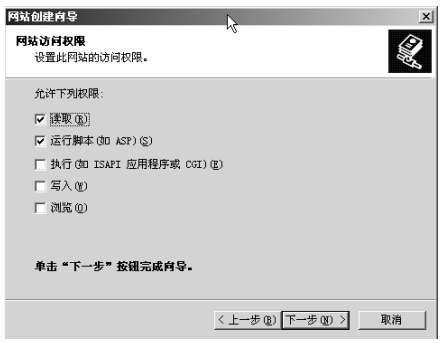

图 3.16　虚拟目录访问权限

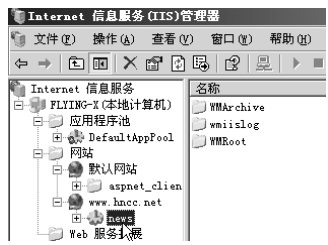

图 3.17　虚拟目录创建完成

如果管理员需要创建多个虚拟目录，使用上面的方法就显得不太方便，这时可以直接在资源管理器中找到需要发布的目录，然后将其设置为 Web 共享，这样也可达到此目的。

（3）创建 NTFS 格式的虚拟目录

① 打开 Windows 资源管理器。

② 右键单击要成为虚拟目录的文件夹，然后单击“共享和安全”按钮，如图 3.18 所示。

③ 单击“Web 共享”选项卡，选择该选项下的“共享文件夹”，如图 3.19 所示。

④ 单击“添加”按钮，在“别名”文本框中，输入虚拟目录的名称，如图 3.20 所示。

⑤ 单击“确定”按钮两次。

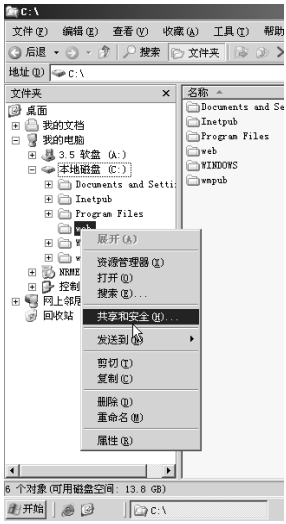

图 3.18　创建 NTFS 格式的虚拟目录

图 3.19　定义 Web 共享

（4）设置默认文档

默认文档是指在浏览器请求指定文档名时提供的文档，它可以是目录的主页或包含站点文档目录列表的索引页。当其他访问者访问管理员的站点时，如果不提供目录下的文档名，则启用默认文档。使用默认文档有利于访问者快速访问站点上的内容，并减少访问者的地址输入工作，因此，管理员应该为每一个主目录和虚拟目录指定默认文档。

启用默认文档的具体操作步骤如下：

① 打开“Internet 信息服务”窗口，在控制台目录树中，需要启用默认文档的 Web 网站或在虚拟目录上单击鼠标右键，在弹出的快捷菜单中选择“属性”命令，在打开的属性对话框中选择“文档”选项卡，如图 3.21 所示。

图 3.20　输入虚拟目录别名

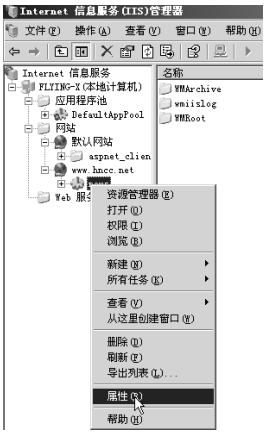

图 3.21　“打开网站属性”对话框

② 在该选项卡中选择“启用默认内容文档”复选框，系统默认的文档为 Default.htm、Default.asp 和 Index.htm。如果管理员要添加一个新的默认文档，可以单击“添加”按钮打开“添加内容页”对话框，在“默认内容页”文本框中输入文档名，然后单击“确定”按钮即可，如图 3.22 所示。

③ 管理员可以通过“添加”按钮指定多个默认文档，系统会按出现在列表框中的名称顺序提供默认文档，并返回所找到的第一个文档。如果要更改搜索顺序，选择一个文档并单击“上移”或“下移”按钮即可，如图 3.23 所示。

图 3.22 “文档”选项卡

图 3.23 “添加内容页”对话框

④ 要从列表框中删除默认文档，单击“删除”按钮即可。

⑤ 默认文档设置完毕，单击“确定”按钮关闭对话框。

【实验四】 虚拟主机技术

【实验步骤】

一般来说，一个主机只能对应一个网站，在这种情况下，会造成主机资源的巨大浪费。所谓虚拟主机，就是让多个独立的网站运行在一台服务器上，把一台运行在网络上的服务器划分成多个“虚拟”的服务器，每一个虚拟主机都具有独立的域名和完整的 Internet 服务器（支持 WWW、FTP、E-mail 等）功能。但一台服务器主机只能够支持一定数量的虚拟主机，当超过这个数量时，用户将会感到性能急剧下降。

在 IIS 中创建虚拟主机的步骤：

（1）通过选择“开始”→“程序”→“管理工具”→“Internet 服务管理器”命令，启动“Internet 信息服务”管理工具，如图 3.24 所示。

（2）鼠标双击在窗口左边列表的“网站”，让其展开，然后在“网站”上单击鼠标右键，依次选择“新建”→“网站”命令，来建立一个虚拟主机，如图 3.25 所示。

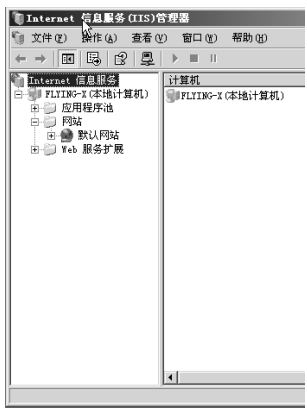

图 3.24 Internet 服务管理器

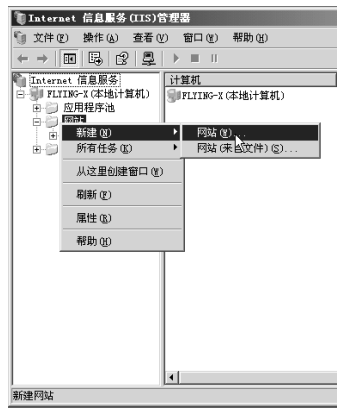

图 3.25 新建虚拟主机

（3）在接着出现的“Web 站点创建向导”，单击“下一步”按钮，并在新出现的窗口中输入所要创建的站点说明，如图 3.26 所示。

（4）在“IP 地址和端口设置”对话框中选择你的 IP 地址，其他端口和主机头项这里使用默认设置即可，如图 3.27 所示。

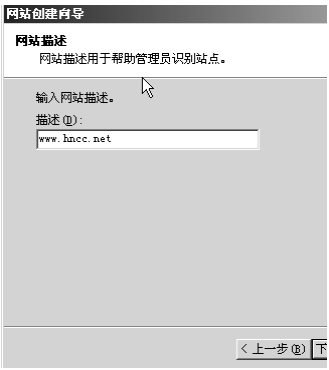

图 3.26　输入站点描述

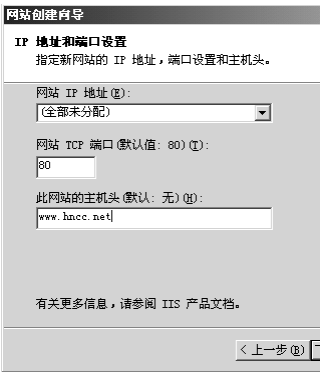

图 3.27　IP 地址、端口、主机头设置

一般来说，可以通过 3 种方法实现在同一台服务器上维护多个站点：分配端口、地址和主机头名。因为每个 Web 站点都具有唯一的、由 3 个部分组成的标识，用来接收和响应请求：端口号、IP 地址、主机头名。通过更改其中的一个标识，就可以在一台计算机上维护多个站点。

① 端口号

通过使用附加端口号，只需一个 IP 地址即可维护多个站点。访问者要访问站点时，需要在 IP 地址后面附加端口号。

② 多 IP 地址

要使用多 IP 地址，必须将主机名及其对应的 IP 地址添加到名称解析系统（通常是 DNS）。此后访问者只需在浏览器中输入文本名称即可访问 Web 站点。如果使用多 IP 地址，则需要为每个 IP 地址附加一块网卡或者为同一块网卡绑定多个 IP 地址。

③ 主机头名

可以使用具有单个静态 IP 地址的主机头名维护多个站点。与以前的方法类似，也需要将主机名添加到名称解析系统（通常是 DNS）。区别在于，一旦请求到达计算机，IIS 将使用在 HTTP 头中传递的主机名来确定客户请求哪个站点。描绘了使用主机头名维护多个 Web 站点的计算机。

（5）单击“下一步”按钮到“Web 站点主目录”设置窗口，其中填入本机上放置网站文件的目录，你也可以通过“浏览”按钮来查找，如图 3.28 所示。

（6）接下来是设置“Web 站点访问权限”，按照默认设置即可，单击“下一步”按钮，在下个窗口中单击“完成”按钮。你已基本建立了一个 Web 站点。下面就可以在你的主目录中放入各种页面文件，让别人在浏览器中输入你的 IP 地址或者域名进行访问了，如图 3.29 所示。

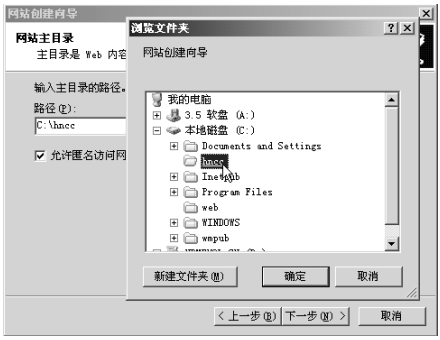

图 3.28　Web 站点主目录

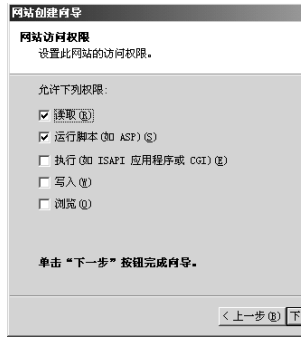

图 3.29　Web 站点访问权限

【实验五】 Web 网站的管理与维护

【实验步骤】

为了使网站有效地运行和提供最新的页面内容，管理员在创建 Web 网站之后，必须对 Web 网站及其他相关内容进行管理，如设置内容过期和分级、启用文档页脚和设置服务器属性等。Web 服务的管理是一个长期而且复杂的工作，管理员需要在实践中逐步地应用和掌握。

在“Internet 信息服务”窗口中，在需要操作的 Web 网站上单击鼠标右键，通过选择快捷菜单中的各项命令，管理员可以对当前站点进行浏览、删除、重命名等各种操作。

一般的管理工作都是通过调整网站的“属性“实现的，可以通过“开始”→“程序”→“管理工具”→“Internet 服务管理器”，启动“Internet 信息服务”管理工具，然后右键单击网站名称，出现快捷菜单，单击“属性”按钮，就可以打开网站属性窗口，如图 3.30 所示。

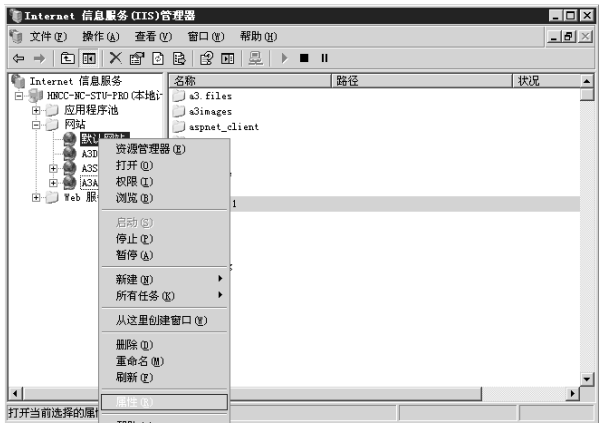

图 3.30　打开网站属性窗口

（1）“网站”选项卡

使用“网站”选项卡可以设置网站的好记名称、配置对网站的访问权限、设置站点的连接限制，以及启用日志记录并配置站点的日志记录格式。

① 网站标识

描述：输入网站的好记名称。好记名称将出现在 IIS 管理器的控制台树中。

IP 地址：从列表框中指定一个 IP 地址或输入用于访问该站点的新 IP 地址。如果没有分配指定的 IP 地址，那么此站点将响应分配给该计算机但没有分配给其他站点的所有 IP 地址，

这使它成为默认网站。要使 IP 地址出现在列表中，必须在控制面板中定义了此 IP 地址均可在该计算机上使用。详细信息，请参阅 Windows Server 2003 家族帮助。站点的描述不是必需的。

TCP 端口：指派运行 Web 服务的 TCP 端口，默认值是端口 80。可以将端口更改成唯一的 TCP 端口号，但是如果更改端口号，则必须预先通知客户端以便请求该更改的端口号，否则它们的请求无法连接到服务器。端口号是必需的，该文本框不能为空。

SSL 端口：指派与该网站标识相关联的 SSL 端口。默认 SSL 端口号是 443。可以将 SSL 端口更改成任何唯一的 TCP 端口号，但要连接到服务器，则必须预先通知客户端以便请求该更改的端口号。只有使用 SSL 加密时才需要 SSL 端口号。如果没有为站点启用 SSL 加密，则“SSL 端口”框不可用。

高级：单击此处可以进一步配置用来访问站点的 IP 地址、TCP 端口号以及主机头值。

② 连接

以秒为单位设置服务器断开不活动用户连接之前的时间长短。这将确保在 HTTP 协议无法关闭某个连接时，关闭所有的连接。大多数 Web 浏览器要求服务器在多个请求中保持连接打开。这称为“保持 HTTP 连接”，它是可以极大地增强服务器性能的 HTTP 规范。如果没有它，浏览器将不得不为包含多个元素（如图形）的页面进行大量的连接请求。可能需要为每个元素进行单独连接。这些额外的请求和连接要求额外的服务器活动和资源，这将会降低服务器的效率。其他请求特别是通过高滞后（慢）连接的请求，也可以使浏览器变慢并且响应变少。在安装过程中，将默认启用保持 HTTP 连接。

连接超时：在框中输入数字（以秒为单位）设置服务器在断开与非活动用户的连接之前等待的时间。这将确保在 HTTP 协议无法关闭某个连接时，关闭所有的连接。

保持 HTTP 连接：选择该选项可以使客户端与服务器保持打开连接，而不是根据每个新请求重新打开客户端连接。禁用“保持 HTTP 连接”可能降低服务器性能。默认情况下启用“保持 HTTP 连接”。

③ 启用日志记录

选择此选项可以启用网站的日志记录功能，它可以记录关于用户活动的细节并按所选格式创建日志。信息存储在 ASCII 文件或与 ODBC 兼容的数据库中。IIS 中的日志记录信息超出了 Microsoft (R) Windows (R) 事件日志或性能监视器功能的范围。日志包括的信息诸如，哪些用户访问了您的站点、访问者查看了什么内容，以及最后一次查看该信息的时间。可以使用日志来评估内容受欢迎程度或识别信息瓶颈。

活动日志格式：在下面的格式中为日志文件选择一种格式：Microsoft IIS 日志文件格式；NCSA 共用日志文件格式；ODBC 日志记录；W3C 扩展日志文件格式。默认情况下选择此格式。要使用进程记账，必须选择 W3SVC 扩展日志文件格式。

属性：单击此处可以配置创建日志文件的选项，或配置 W3C 扩展日志或 ODBC 日志的属性。“网站”选项卡如图 3.31 所示。

（2）“性能”选项卡

使用“性能”选项卡可以设置影响带宽使用的属性，以及客户端 Web 连接的数量。通过配置给定站点的网络带宽，可以更好地控制该站点允许的流量。例如，通过限制低优先级的网站上的带宽和/或连接数，可以允许其他高优先级站点处理更多的流量负载。设置是站点特定的，并可随着网络流量和使用情况的改变而进行调整。

① 带宽限制

带宽限制限制了该网站可用的带宽。当发送数据包时，带宽限制使用数据包计划程序进行管理。当使用 IIS 管理器将站点配置成使用带宽限制时，系统将自动安装数据包计划程序，并且 IIS 自动将带宽限制设置成最小值 1024 字节/秒。

限制网站可以使用的网络带宽：选择该选项可以启用网站的带宽限制。

最大带宽：在框中输入或单击向上和向下箭头来设置希望该网站可用的最大带宽（千字节/秒）。

② 网站连接

您可以将 Internet 信息服务（IIS）配置成允许数目不受限制的并发连接，或限制该网站接收的连接个数。如果连接趋向于波动，则将数量设置成不受限制可以避免常量管理。但是，如果连接数超过了系统资源，则系统性能可能受到影响。将站点限定在特定的连接数可以保持性能的稳定。设置是站点特定的，并且可以随着网络流量和使用情况的改变而进行调整。

不受限制：单击此处可以将网站配置成处理不限制数量的并发连接。

连接限制为：单击此处可以设置该网站的特定数目的并发连接。在框中输入数值或单击向上和向下箭头来设置连接的数量，如图 3.32 所示。

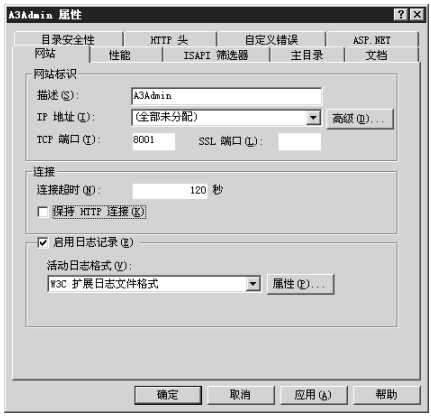

图 3.31 “网站”选项卡

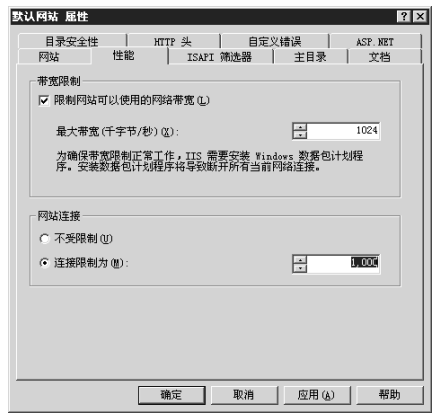

图 3.32 “网站性能”选项卡

（3）“ISAPI 筛选器”选项卡

使用“ISAPI 筛选器”选项卡可以设置 ISAPI 筛选器选项。ISAPI 筛选器是在处理 HTTP 请求过程中响应事件的程序。表中列出了每个筛选器的状态（可以启动或禁用）、文件名，以及加载到内存的优先级。只能更改具有相同优先级的筛选器的执行顺序。如果在共用层添加或更改筛选器，则必须重新启动 Internet 信息服务（IIS）以加载新的筛选器。如果在网站级别添加或更改筛选器，则只有当网站请求时才能加载该筛选器。

① 添加。单击“添加”按钮可以通过浏览可执行文件和提供友好名称来添加现有的 ISAPI 筛选器。

② 删除。单击“删除”按钮可以从该加载列表中删除当前所选的 ISAPI 筛选器。

③ 编辑。单击“编辑”按钮可以修改当前所选的 ISAPI 筛选器的属性。

④ 应用。单击“应用”按钮可以阻止加载当前所选的 ISAPI 筛选器，但将其保留在筛选器列表中。

⑤ 上移。单击“上移”按钮可以将当前所选的筛选器移到执行顺序中的更高位置。

⑥ 下移。单击“下移”按钮可以将当前所选的筛选器移到执行顺序中的较低位置，如图 3.33 所示。

（4）“主目录”选项卡

使用“主目录”选项卡可以在 IIS 服务器上创建和管理网站。此选项卡上的设置与虚拟目录的主目录选项卡上的可用设置相似。

在设置本地或网络路径时，允许将请求重定向到正确的物理位置。通过设置用户访问权限，选择是否记录对这些资源的请求，以及选择是否使用索引服务索引该站点，并可以进一步配置物理位置。要指定何时接收请求，必须对应用程序进行标识、定位并给予适当的执行权限和保护。

① 此资源的内容来自

此计算机上的目录：单击此单选按钮可以允许用户访问该计算机上的指定目录，以便查看或更新 Web 内容。可以在“本地路径”文本框中输入目录名称。

另一台计算机上的共享：单击此单选按钮可以允许用户查看或更新与该计算机有活动连接的其他计算机上的 Web 内容。在选中后，可以在“网络目录”框中输入服务器名和目录名。单击“连接为”按钮可以输入网络用户名和密码信息。

重定向到 URL：单击此单选按钮可以通过在“重定向到”框中输入 URL，将客户端应用程序（如浏览器）重定向到其他网站或虚拟目录。在选中后，重定向选项将替代路径选项。

② 应用程序设置

在 Web 开发中，网站和应用程序的代码十分复杂并且不断变化。网站和应用程序每周、每个月都在改变。因此，在保护应用程序和管理性能的同时，需要控制那些主动管理运行时环境的服务。

应用程序名：输入根目录的名称，该目录中包含了应用程序的文件和子目录。

开始位置：显示应用程序在其上配置的配置数据库节点。

执行权限：此选项确定该站点资源的许可的程序执行级别。将权限设置为“无”可以限制只能访问静态文件，如 HTML 或图像文件。将权限设置为“纯脚本”可以只允许运行纯脚本，而不运行可执行程序，将权限设置为“脚本和可执行文件”可以删除所有限制，以便所有文件类型均可以访问或执行。

应用程序池：单击列表框中与该主目录相关联的应用程序池。

删除或创建：单击此按钮可以从网站删除或创建应用程序，同时保持虚拟目录不变。

配置：单击此按钮可以配置应用程序映射、选项和调试功能。

卸载：单击此处可以从内存卸载隔离的应用程序，或者卸载没有被其他应用程序引用的汇集应用程序，如图 3.34 所示。

（5）“文档”选项卡

使用“文档”选项卡可以定义站点的默认网页并在站点文档中附加页脚。

① 启用默认内容文档

启用后，只要浏览器请求没有指定的文档名称，则将默认文档提供给浏览器。默认文档可以是目录主页或包含站点文档目录列表的索引页。多个文档可以按照自上向下的搜索顺序列出。此处显示的文件可在站点的主目录中找到。单击“上移”和“下移”按钮可以修改顺序。启用默认内容文档复选框可以使 Web 服务器识别默认文档（只要浏览器请求没有指定文档名称）。

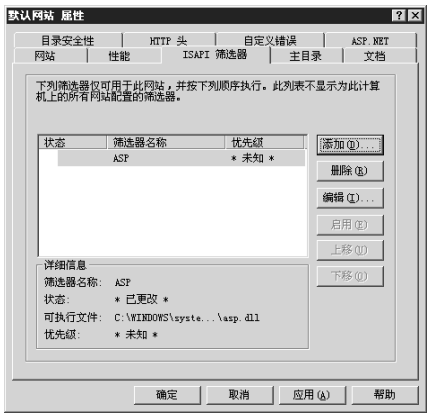

图 3.33 “ISAPI 筛选器”选项卡

图 3.34 “主目录”选项卡

添加：单击此按钮可以添加其他默认文档。按照在列表中显示的名称顺序依次提供默认文档。服务器将返回找到的第一个文档。

删除：单击此按钮可以从列表中删除默认文档而不删除文件。

② 启用文档页脚

选择“启用文档页脚”复选框可以将 Web 服务器配置成自动附加页脚到 Web 服务器返回的所有文档中。页脚文件不应该是完整的 HTML 文档。它应该只包含格式化页脚内容的外观和功能时必要的 HTML 标记。

浏览：单击此按钮可以查找和指定页脚文件的完整路径和文件名，如图 3.35 所示。

（6）“目录安全性”选项卡

使用“目录安全性”选项卡设置 IIS 安全性功能，可以在授权访问受限制的内容之前确认用户的用户标识。

① 身份验证和访问控制

该设置允许其配置 Web 服务器，使其在指派受限内容的访问权限之前确认用户的用户标识。但是，必须先创建有效的 Windows 用户账户然后配置这些账户的 NTFS 目录和文件访问权限，Web 服务器才能验证用户的身份。

编辑：单击此按钮可以配置 Web 服务器的身份验证和匿名访问功能。

② IP 地址和域名限制

该设置基于 IP 地址或域名允许其指派或拒绝特定用户、计算机、计算机组，或域访问该网站、目录或文件。

编辑：单击此按钮可以添加设置限制或拒绝特定用户、计算机、计算机组，或域对该网站、目录或文件的访问的设置。

③ 安全通信

Windows 通过使用服务器证书和证书映射来提供保护客户端与 Web 服务器之间通信安全的途径。可以通过启用 Windows 目录服务映射来实现安全通信，该服务映射允许其使用目录服务客户端证书映射，而不是一对一或多对一映射。要启用该服务，服务器必须是 Windows (R) Server 2003 域的成员。

服务器证书：单击此按钮可以启动“Web 服务器证书向导”并获取服务器证书。

查看证书：单击此按钮可以查看该网站服务器证书（如果已安装的话）。

编辑：单击此按钮可以启用通信设置，如证书接收、证书映射及证书信任列表，如图 3.36 所示。

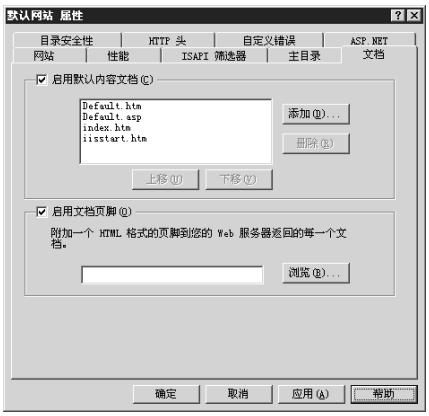

图 3.35 “文档”选项卡

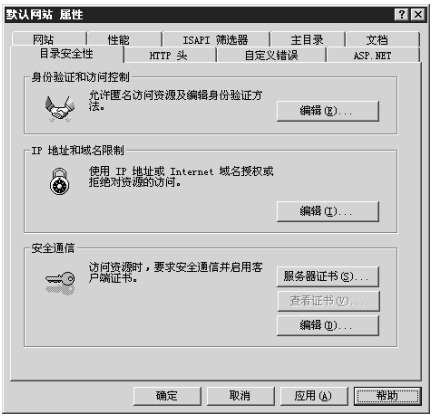

图 3.36 “目录安全性”选项卡

（7）“HTTP 头”选项卡

使用“HTTP 头”选项卡可以在 HTML 页的标题中设置返回到浏览器的值。也可以设置内容的内容分级，以及定义 MIME 类型。这些值可以对所有站点进行全局设置，也可以在每个站点中单独设置。Internet 信息服务（IIS）对这些设置使用继承模型。如果设置或更改了与层次结构中的其他节点处的设置有冲突的设置，那么系统将提示您指定应用此新设置的节点。

① 启用内容过期

对于对时间敏感的材料（如特定的报价或事件公告），可以选择“启用内容过期”复选框以包括过期信息。浏览器将当前日期与过期日期相比较，以决定是显示一个缓存页，还是从服务器请求一个更新的页面。

立即过期：单击此选项后内容将立即过期。该设置强制浏览器总是从服务器上检索有关后续请求的最新内容。

此时间段后过期：设置特定的时间段。若是超过该时间段后，则强制浏览器重新从服务器上检索有关后续请求的内容。

过期时间：选择此选项可以设置特定的日期和时间。若是超过该日期和时间后，则强制浏览器重新从服务器上检索有关后续请求的内容。

② 自定义 HTTP 头

可以使用该属性将自定义 HTTP 头从 Web 服务器发送到客户端浏览器。自定义头可用来将当前 HTTP 规范中尚不支持的指令从 Web 服务器发送到客户端，如产品发布时 IIS 尚不支持的更新的 HTTP 头。例如，可以使用自定义 HTTP 头来允许客户端浏览器缓存页面而禁止代理服务器缓存页面。

添加：单击此按钮可以添加新的自定义 HTTP 头。

编辑：单击此按钮可以编辑当前所选的自定义 HTTP 头的属性。

删除：单击此按钮可以删除当前所选的自定义 HTTP 头。

③ 内容分级

使用内容分级在网页的 HTTP 头中嵌入描述性的标签。浏览器（如 Microsoft（R）Internet Explorer 3.0 或更高版本）可以检测内容分级，以帮助用户识别潜在的令人反感的 Web 内容。

编辑分级：单击此按钮可以设置内容分级值。

④ MIME 类型

多用途 Internet 邮件扩展（MIME）映射设置了 IIS 用于服务客户端的各种文件类型。IIS 仅为扩展名在 MIME 类型列表中注册过的文件提供服务。可对 IIS 全局定义 MIME 类型，并且可以在网站、网站目录及网站虚拟目录级别上定义其他的 MIME 类型。IIS 对 MIME 类型设置使用继承模型。所有网站、网站目录，以及网站虚拟目录继承在共用层定义的 MIME 类型。在网站、网站目录，或网站虚拟目录处定义的 MIME 类型仅用于特定的节点上。如果设置或更改了层次结构中与另一个节点的设置相冲突的 MIME 类型，则“继承覆盖”对话框将进行提示，您可以在该对话框中指定应用新设置的节点。“注册的 MIME 类型（文件扩展名）”列表框中列出了安装在该计算机上的已注册的文件类型。

MIME 类型：单击此处可以配置 MIME 映射。这些映射对 Web 服务返回给浏览器的不同文件类型进行设置，如图 3.37 所示。

（8）“自定义错误”选项卡

使用“自定义错误”选项卡可以自定义 HTTP 错误信息，当 Web 服务器发生错误时，将此错误信息发送给客户端。管理员可以使用 IIS 提供的一般默认 HTTP 1.1 错误或详细的自定义错误文件，或者创建自己的自定义错误文件。这些值可以对所有站点进行全局设置，也可以在每个站点中单独设置。IIS 对于这些设置使用继承模型。如果你设置或更改了与层次结构中的其他节点处的设置有冲突的设置，那么系统将提示你指定应用此新设置的节点。

编辑：单击此按钮可以更改当前所选的自定义错误信息的属性。

设为默认值：单击此按钮可以将当前所选的自定义错误信息配置成使用默认的 HTTP 1.1 错误，如图 3.38 所示。

图 3.37 “HTTP 头”选项卡

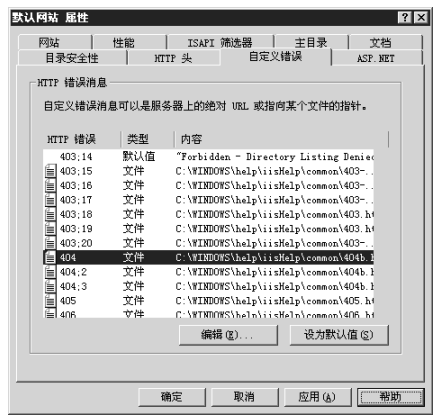

图 3.38 “自定义错误”选项卡

【总结】

利用 Wiondws 2003 自带的 IIS 平台，可以方便、快捷的搭建一个 Web 服务器，但是安全性不是很高，为了构建安全的 Web 服务器，还需要进行相应的设置。

思考：

1．分析出错现象：HTTP 错误 404.文件或目录未找到。

2．分析出错现象：HTTP 错误 401.2.未经授权：访问由于服务器配置被拒绝。

3．分析出错现象：类似于 Server.MapPath()错误“ASP0175:80004005”的出错信息。

任务二　使用 Apache 架设企业网站

3.2.1　任务目的

熟悉 Apache 服务器，在 Windows Server 2003 下构建一个 Apache 服务器，利用 Apache 服务器发布网站。

3.2.2　任务描述

在 Windows Server 2003 系统上安装一个 Apache 服务器，并且进行简单的设置。

3.2.3　相关基础知识

Apache 是一种开放源码的 HTTP 服务器，可以在大多数计算机操作系统中运行，由于其多平台和安全性被广泛使用，是最流行的 Web 服务器端软件之一。它快速、可靠并且可通过简单地 API 扩展，Perl/Python 等解释器可被编译到服务器中。

Apache 起初由 Illinois 大学 Urbana-Champaign 的国家高级计算程序中心开发。此后，Apache 被开放源代码团体的成员不断地发展和加强。Apache 服务器拥有牢靠、可信的美誉，已用在超过半数的互联网站中，特别是几乎所有最热门和访问量最大的网站。

最初，Apache 只是 Netscape 网页服务器（现在是 Sun ONE）之外的开放源代码选择。渐渐地，它开始在功能和速度。超越其他的基于 UNIX 的 HTTP 服务器。1996 年 4 月以来，Apache 一直是 Internet 上最流行的 HTTP 服务器，1999 年 5 月，它在 57%的网页服务器上运行；到了 2005 年 7 月，这个比例上升到了 69%。

Apache 支持许多特性，大部分通过编译的模块实现。这些特性从服务器端的编程语言支持到身份认证方案。一些通用的语言接口支持 Perl、Python、Tcl 和 PHP。流行的认证模块包括 mod_access、mod_auth 和 mod_digest。其他的例子有 SSL 和 TLS 支持（mod_ssl）、proxy 模块，很重要的 URL 重写（由 mod_rewrite 实现），定制日志文件（mod_log_config），以及过滤支持（mod_include 和 mod_ext_filter）。Apache 日志可以通过网页浏览器使用免费的脚本 AWStats 或 Visitors 来进行分析。

Apache 的 2.x 版本核心在 Apache 1.x 版本之上做出了重要的加强。包括：线程、更好的支持非 UNIX 平台（如 Windows）、新的 Apache API，以及 IPv6。

3.2.4　实现参考

实验环境

Windows Server 2003 企业版。

【实验一】 安装 Apache 软件

【实验步骤】

（1）单击安装文件，出现安装向导界面如图 3.39 所示。单击“Next”按钮进入安装许可条例界面。

（2）安装许可条例界面如图 3.40 所示。单击“Next”按钮进入使用须知界面如图 3.41 所示。

（3）在使用须知界面单击“Next”按钮进入服务器信息界面，如图 3.42 所示。

图 3.39　安装向导界面

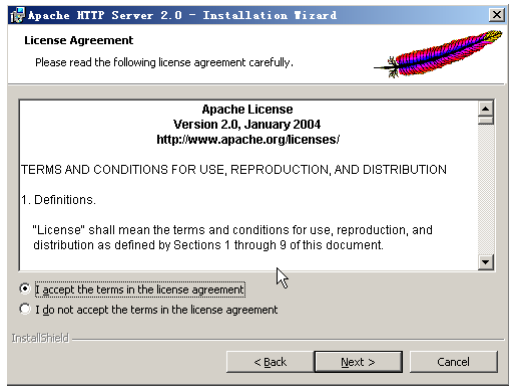

图 3.40　安装许可条例界面

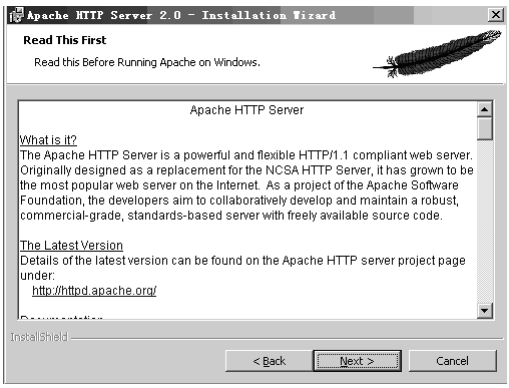

图 3.41　使用须知界面

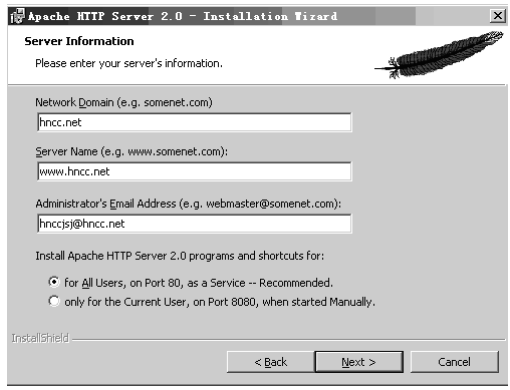

图 3.42　服务器信息界面

在图 3.42 所示服务器信息对话框中，依次填入的是“域名”、“服务器名称”、“系统管理员邮件地址”。三条信息均可任意填写，下面有两个选择，但图片上选择的是为系统所有用户安装，使用默认的 80 端口，并作为系统服务自动启动；另外一个是仅为当前用户安装，使用端口 8080，手动启动。一般选择如图 3.43 所示。单击“Next”按钮继续。选择“Custom”用户自定义安装。单击“Next”按钮进入安装选择对话框。

（4）图 3.43 是选择安装对话框。在对话框中单击“Apache HTTP Server 2.0.63”，选择“This feature, and all subfeatures, will be installed on local hard drive.”，即“此部分，以及下属子部分内容，全部安装在本地硬盘上”。单击“Change...”按钮，手动指定安装目录。一般建议不要安装在操作系统所在盘，以免操作系统损坏之后，还原操作把 Apache 配置文件也清除了。单击“OK”按钮继续。进入图 3.44 所示界面。

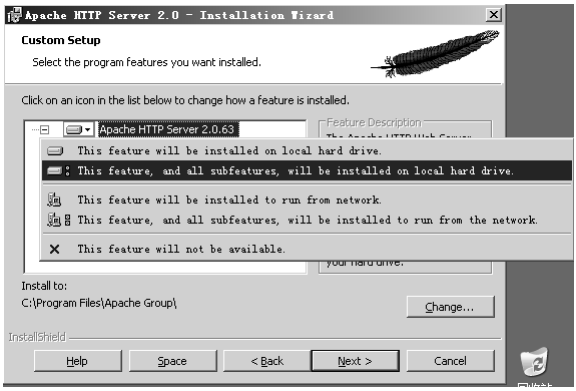

图 3.43　选择安装界面

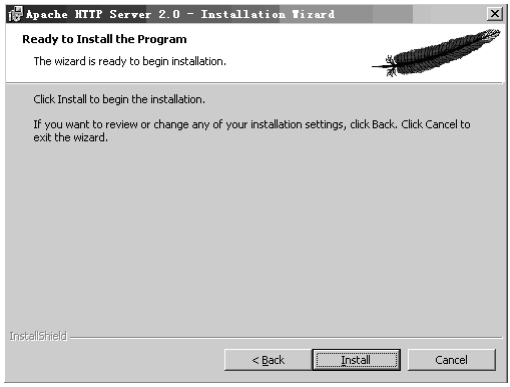

图 3.44　确认安装界面

（5）图 3.44 是确认安装界面。确认安装选项无误，如果认为要再检查一遍，可以单击“Back”按钮一步步返回检查。单击“Install”按钮开始按前面设定的安装选项安装，安装完成后进入图 3.45 所示界面，单击“Finsh”按钮完成安装。

（6）安装完成后，在桌面的右下角有绿色图标，表示 Apache 服务器开始运行。为了测试安装是否成功，在 IE 地址栏打开“http://127.0.0.1”，单击“转到”，就可以看到图 3.46 所示界面，表示 Apache 服务器已安装成功。

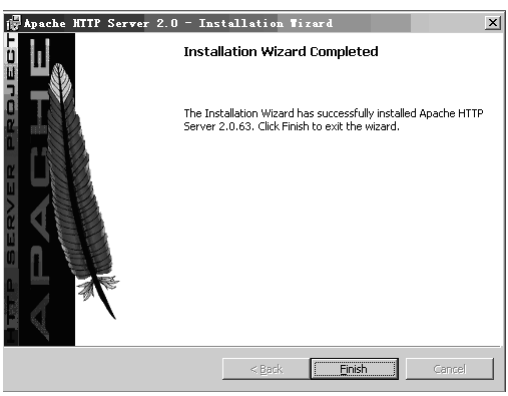

图 3.45　安装完成

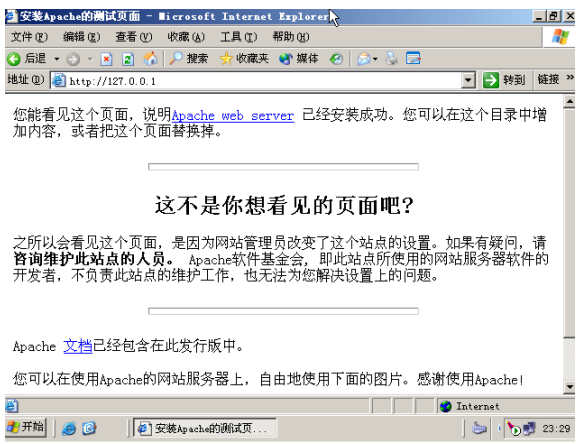

图 3.46　安装成功

【实验二】 简单配置 Apache 服务器

【实验步骤】

（1）修改网站默认目录。如果不配置 Apache 服务器，你的安装目录下的 Apache2\htdocs 文件夹即网站的默认根目录，在里面放入文件就可以了。如果要修改，选择“开始”→“所有程序”→“Apache HTTP Server 2.0”→“Configure Apache Server”→“Edit the Apache httpd conf Configuration file”命令。在打开的记事本中定位到 Ln228 行，或者查找关键字“DocumentRoot”（网站根目录），找到图 3.47 所示配置文件，将`"E:/insoft/Apache2/htdocs"` 内的地址改成你的网站根目录，地址格式按照图上所写，一般文件地址的“\”在 Apache 里要改成“/”。

（2）在文本中定位到 Ln321，找到 DirectoryIndex（目录索引，即在仅指定目录的情况下，

默认显示的文件名），如图 3.48 所示，在 DirectoryIndex 后可以添加很多默认文档名，系统会根据从左至右的顺序来优先显示，以单个半角空格隔开，如有些网站的首页是 index.htm，可以在光标那里加上“index.htm”，文件名是任意的，不一定必须是“index.html”，如“test.php”等都可以。

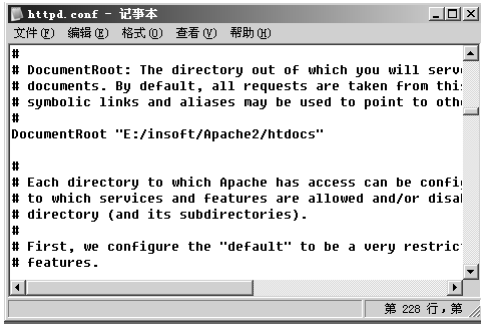

图 3.47　配置文件

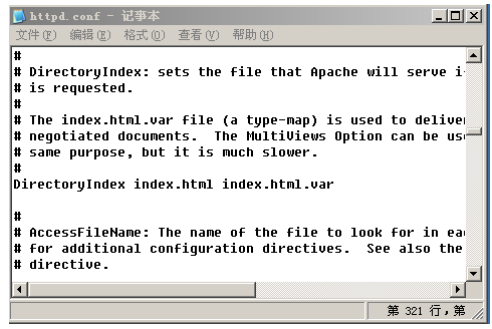

图 3.48　默认文档

项目 4

部署 DNS 服务

学习目标

DNS 是域名系统（Domain Name System）的缩写，该系统用于命名组织到域层次结构中的计算机和网络服务。在 Internet 上域名与 IP 地址之间是一一对应的，域名虽然便于人们记忆，但机器之间只能互相认识 IP 地址，它们之间的转换工作称为域名解析，域名解析需要由专门的域名解析服务器来完成，DNS 就是进行域名解析的服务器。

- 认识 DNS；
- 理解 DNS 的查询过程；
- 掌握 Windows 2003 操作系统平台下构建 DNS 服务；
- 掌握 Linux 操作系统平台下构建 DNS 服务；
- 掌握智能 DNS 服务平台构建。

内容框架

项目 4 的内容框架如图 4.1 所示。

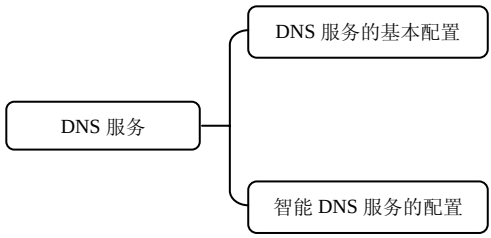

图 4.1　内容框架

任务一　Windows Server 2003 部署 DNS 服务

4.1.1　任务目的

本任务的目的在于掌握 Windows Server 2003 DNS 服务的安装和设置方法，从而对 DNS

的概念和结构有一定的认知。

4.1.2 任务描述

将安装了 Windows Server 2003 企业版的计算机配置成 DNS 服务器。

4.1.3 相关基础知识

DNS 是域名系统（Domain Name System）的缩写，该系统用于命名组织到域层次结构中的计算机和网络服务。在 Internet 上域名与 IP 地址之间是一一对应的，域名虽然便于人们记忆，但机器之间只能互相认识 IP 地址，它们之间的转换工作称为域名解析，域名解析需要由专门的域名解析服务器来完成，DNS 就是进行域名解析的服务器。

（1）域名结构

Internet 的域名结构是由 TCP/IP 协议集的域名系统（Domain Name System，DNS）定义的。域名系统与 IP 地址的结构一样，采用层次结构。域名系统将整个 Internet 划分为多个顶级域，顶级域的划分采用了两种划分模式，即组织模式和地理模式。

域名系统中，组织模式有 7 个顶级域，见表 4-1。

表 4-1 域名系统组织模式

顶 级 域 名	分 配 给
com	商业组织
edu	教育机构
gov	政府部门
mil	军事部门
net	主要网络支持中心
org	上述以外的组织
int	国际组织

例如，当看到 www.ibm.com 这个名字时，因其顶级域名为 com，所以推知 IBM 是一家公司，而 www.ibm.com 可能是一个公司的网站地址。

地理模式的顶级域是按照国家或地区进行划分的，每个申请接入 Internet 的国家或地区都可以作为一个顶级域出现。如 cn 代表中国，jp 代表日本，fr 代表法国，uk 代表英国，ca 代表加拿大等。

网络信息中心将顶级域的管理权授予指定的管理机构，各个管理机构再为它们所管理的域分配二级域名，并将二级域名的管理权授予其下属的管理机构，如此层层细分，就形成了 Internet 层次状的域名结构。

Internet 主机域名的排列原则是低层的子域名在前面，而它们所属的高层域名在后面。Internet 主机域名的一般格式为：

四级域名．三级域名．二级域名．顶级域名

在域名系统 DNS 中，每个域是由不同的组织来管理的，而这些组织又可将其子域分给其

他的组织来管理。这种层次结构显示出众多优点，如各个组织在它们的内部可以自由的选择域名，只要保证组织内的唯一性，而不用担心与其他组织内的域名冲突。

在 Internet 中，对应于域名结构，名字服务器也构成一定的层次结构，如图 4.2 所示。这个树形的域名服务器的逻辑结构是域名解析算法赖以实现的基础。总的来说，域名解析采用自顶向下的算法，从根服务器开始直到叶服务器，在其间的某个节点上一定能找到所需的名字——地址映射。当然，由于父子节点的上下管辖关系，名字解析的过程只需走过一条从树中某节点开始到另一节点的一条自顶向下的单向路径，无须回溯，更不用遍历整个服务器树。

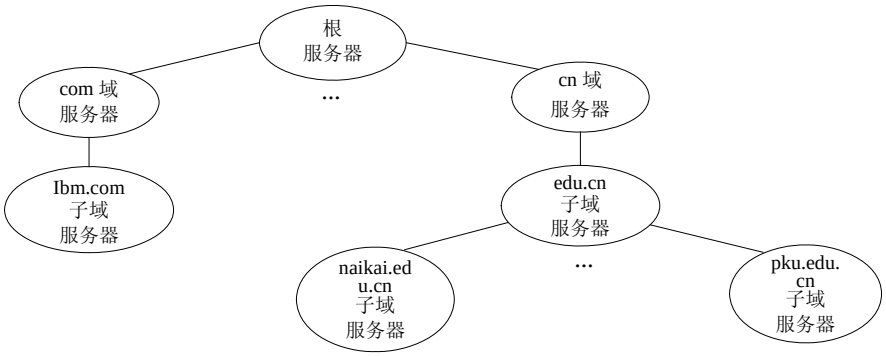

图 4.2　名字服务器层次结构示意图

（2）区域

为了便于根据实际情况来分散 DNS 名称管理工作的负荷，将 DNS 名称空间划分为区域（zone）来进行管理。区域是 DNS 服务器的管辖范围，是由 DNS 名称空间中的单个区域或由具有上下隶属关系的紧密相邻的多个子域组成的一个管理单位。因此，DNS 名称服务器是通过区域来管理名称空间的，而并非以域为单位来管理名称空间，但区域的名称与其管理的 DNS 名称空间的域的名称是一一对应的。

一台 DNS 服务器可以管理一个或多个区域，而一个区域也可以由多台 DNS 服务器来管理（例如，由一个主 DNS 服务器和多个辅助 DNS 服务器来管理）。在 DNS 服务器中必须先建立区域，然后再根据需要在区域中建立子域及在区域或子域中添加资源记录，才能完成其解析工作。

（3）DNS 解析过程

通常，请求域名解析的软件知道如何访问一个服务器，而每一域名服务器都至少知道根服务器地址及其父节点服务器地址。域名解析有两种方式，一种叫递归解析，一般客户机和服务器之间属递归查询，即当客户机向 DNS 服务器发出请求后，若 DNS 服务器本身不能解析，则会向另外的 DNS 服务器发出查询请求，得到结果后转交给客户机。另一种叫循环解析，每次请求一个服务器，不行再请求别的服务器。图 4.3 描述了一个简单的名字解析流程图。

4.1.4　实现参考

实验环境

Windows Server 2003 企业版。

【实验一】 安装 Windows Server 2003 企业版 DNS 网络服务组件

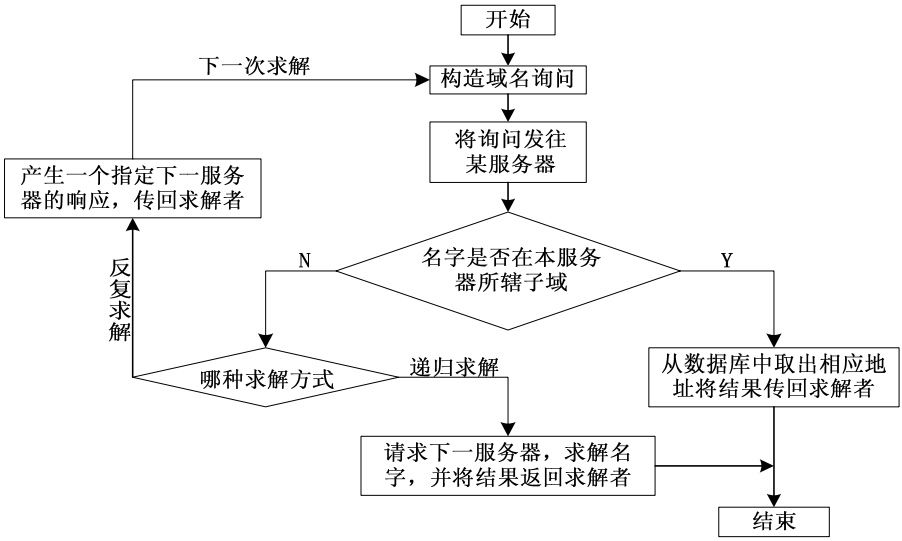

图 4.3　名字解析流程图

完成 Windows Server 2003 企业版的默认安装后，需要手动安装和配置 DNS 服务，这是因为 DNS 网络服务组件不是默认安装组件。

【实验步骤】

（1）依次选择“开始”→“管理工具”→“配置您的服务器向导”命令，在打开的向导页中单击“下一步”按钮。配置向导自动检测所有网络连接的设置情况，若没有发现问题则进入“服务器角色”向导页，如图 4.4 所示。

小提示：如果是第一次使用配置向导，则还会出现一个“配置选项”向导页，选择“自定义配置”单选框即可。

（2）在“服务器角色”列表中单击“DNS 服务器”选项，如图 4.5 所示，并单击“下一步”按钮。打开“选择总结”向导页，如果列表中出现“安装 DNS 服务器”和“运行配置 DNS 服务器向导来配置 DNS”，则直接单击“下一步”按钮。否则单击“上一步”按钮重新配置。

图 4.4　配置服务器向导

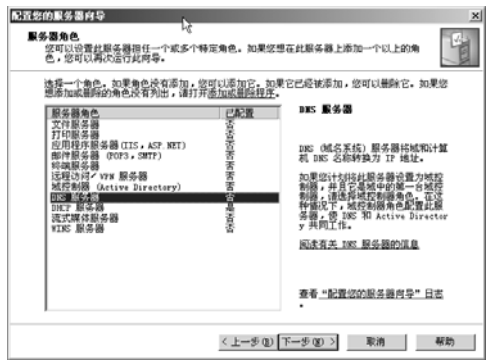

图 4.5　选择“DNS 服务器”选项

（3）向导开始安装 DNS 服务器，并且可能会提示插入 Windows Server 2003 的安装光盘或指定安装源文件，如图 4.6 所示。

小提示：如果该服务器当前配置为自动获取 IP 地址，则“Windows 组件向导”的“正在配置组件”页面就会出现，提示用户使用静态 IP 地址配置 DNS 服务器。

【实验二】 创建一个正向搜索区域

DNS 服务器安装完成以后会自动打开“配置 DNS 服务器向导”对话框。用户可以在该向导的指引下创建正向搜索区域。

所谓正向搜索区域是指将域名解析为 IP 地址的过程。也就是说，当用户输入一个服务器域名时，借助于该记录可以将域名解析为 IP 地址，从而实现对服务器的访问。

【实验步骤】

（1）在“配置 DNS 服务器向导”的欢迎页面中单击“下一步”按钮，打开“选择配置操作”向导页。在默认情况下适合小型网络使用的“创建正向查找区域”单选框处于选中状态。因此保持默认选项并单击“下一步”按钮，如图 4.7 所示。

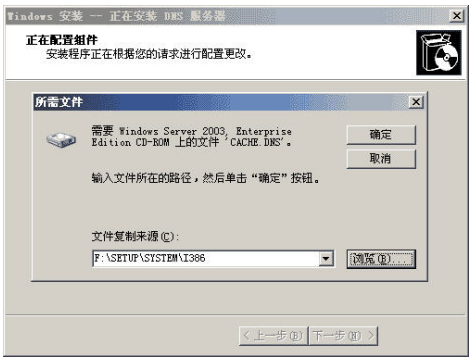

图 4.6　指定系统安装盘或安装源文件

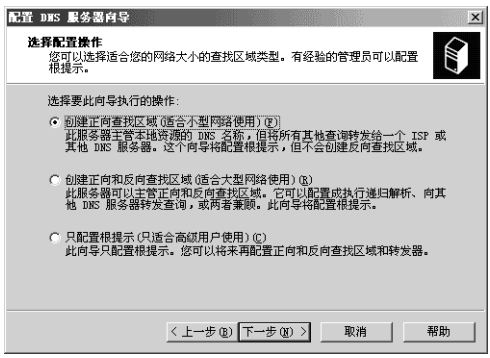

图 4.7　选择配置操作

（2）打开“主服务器位置”向导页，如果所部署的 DNS 服务器是网络中的第一台 DNS 服务器，则应该保持“这台服务器维护该区域”单选框的选中状态，将该 DNS 服务器作为主 DNS 服务器使用，并单击“下一步”按钮，如图 4.8 所示。

（3）打开“区域名称”向导页，在“区域名称”编辑框中输入一个能反映公司单位信息的区域名称（如“hncc.net”），单击“下一步”按钮，如图 4.9 所示。

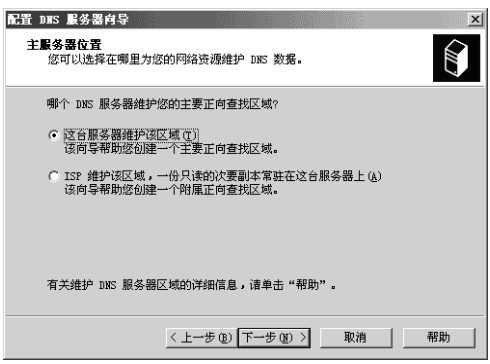

图 4.8　确定主服务器的位置

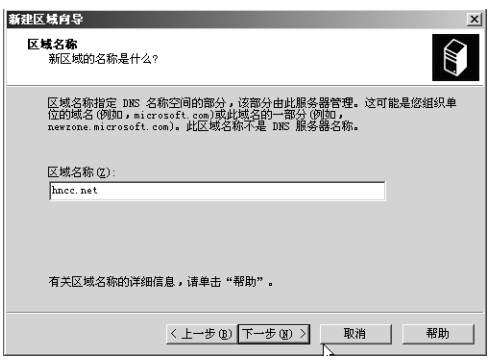

图 4.9　填写区域名称

（4）在打开的“区域文件”向导页中已经根据区域名称默认填入了一个文件名。该文件是一个 ASCII 文本文件，里面保存着该区域的信息，默认情况下保存在“c:\windows\system32\DNS”文件夹中。保持默认值不变，单击“下一步”按钮，如图 4.10 所示。

（5）在打开的“动态更新”向导页中指定该 DNS 区域能够接收的注册信息更新类型。允许动态更新可以让系统自动地在 DNS 中注册有关信息，在实际应用中比较有用，因此选择“允许非安全和安全动态更新”单选框，单击“下一步”按钮，如图 4.11 所示。

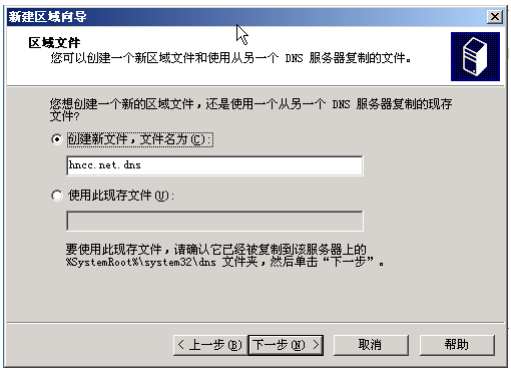

图 4.10　创建区域文件

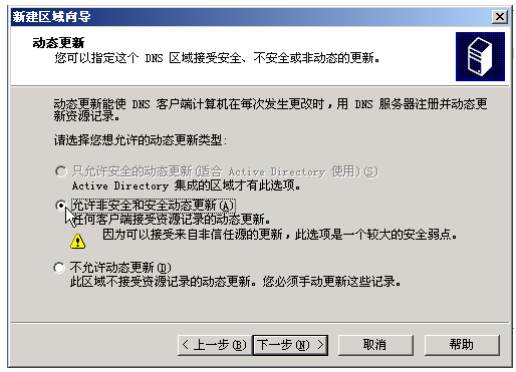

图 4.11　选择允许动态更新

（6）打开“转发器”向导页，选择“是，应当将查询转发到有下列 IP 地址的 DNS 服务器上”单选框。在 IP 地址编辑框中输入 ISP（或上级 DNS 服务器）提供的 DNS 服务器 IP 地址，单击“下一步”按钮，如图 4.12 所示。

小提示：通过配置“转发器”可以使内部用户在访问 Internet 上的站点时使用当地的 ISP 提供的 DNS 服务器进行域名解析。

（7）依次单击“完成”按钮结束，“hncc.net”区域的创建过程和 DNS 服务器的安装配置过程。

【总结】

在本案例中，要理解区域名的概念，在设置“转发器”时，一定要设置自己所有 ISP 的 DNS 服务器地址，这样可以增加 DNS 查询成功的概率。

【实验三】 创建域中的一个主机名称

利用向导成功创建了“hncc.net”区域，可是内部用户还不能使用这个名称来访问内部站点，因为它还不是一个合格的域名。接着还需要在其基础上创建指向不同主机的域名才能提供域名解析服务。例如，创建一个用以访问 Web 站点的域名 www.hncc.net。

【实验步骤】

（1）依次选择“开始”→“管理工具”→“DNS”菜单命令，打开“dnsmgmt”控制台窗口，如图 4.13 所示。

（2）在左窗格中依次展开“FLYING-X”→“正向查找区域”目录。然后右键单击“hncc.net”区域，执行快捷菜单中的“新建主机”命令，如图 4.14 所示。

在名称对话框中输入新建主机的名称，一般 Web 服务器都是用 www 命名，可选择是否创建相关指针。最后单击“添加主机”按钮结束创建，如图 4.15 所示。

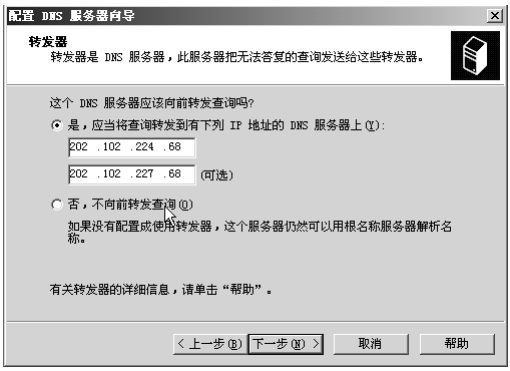

图 4.12　配置 DNS 转发图

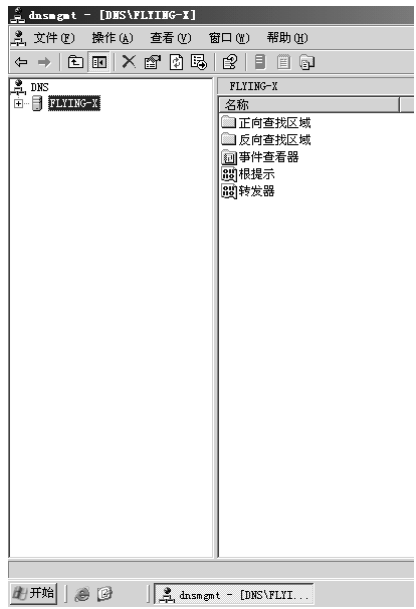

图 4.13　dnsmgmt 控制台窗口

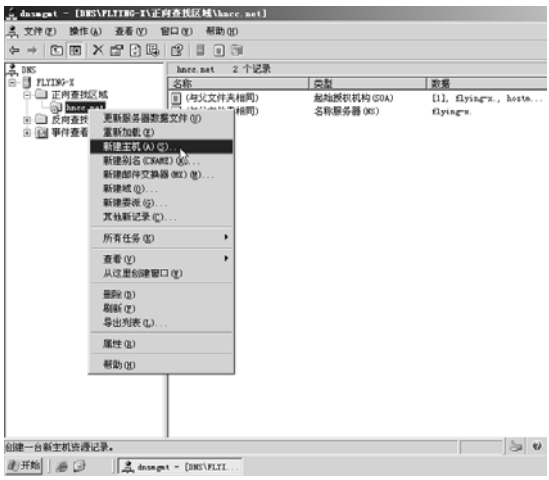

图 4.14　执行“新建主机”命令

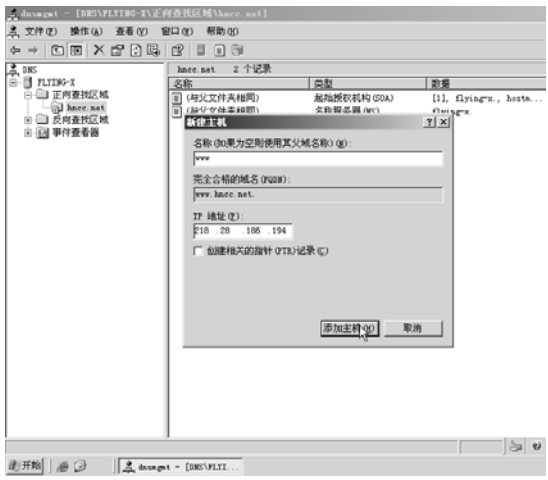

图 4.15　创建主机记录

【实验四】 创建 DNS 域的反向搜索区域

所谓反向搜索区域就是从 IP 地址解析为域名，在大部分的 DNS 搜索中，客户机一般执行正向搜索。DNS 同时提供反向搜索，允许客户机根据一台计算机的 IP 地址搜索它的 DNS 名称。反向搜索的域名信息保存在反向搜索区域中。为进行反向搜索，需要在 DNS 服务器中创建反向搜索区域。

【实验步骤】

（1）选择“开始”→“管理工具”→“DNS”菜单命令，打开“dnsmgmt”控制台窗口。

（2）在左窗格中依次展开“FLYING-X”→“反向查找区域”目录。然后右键单击“反向查找区域”区域，执行快捷菜单中的“新建区域”命令，如图 4.16 所示。

（3）在出现的区域类型窗口中，选择“主要区域”，然后单击“下一步”按钮，如图 4.17

所示。

图 4.16　新建反向查找区域

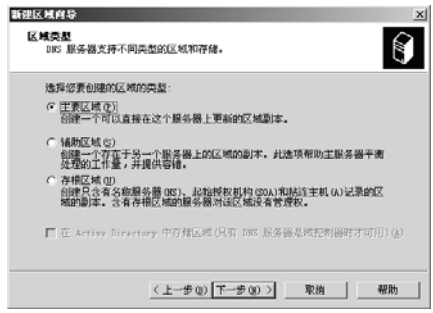

图 4.17　新建主要区域

（4）在出现的“反向查找区域名称”窗口中的“网络 ID”复选框中输入“218 .28 .186 .”域名对应的 IP 地址的网络号，然后单击“下一步”按钮，如图 4.18 所示。

（5）在出现的“区域文件”窗口中，直接单击“下一步”按钮，如图 4.19 所示。

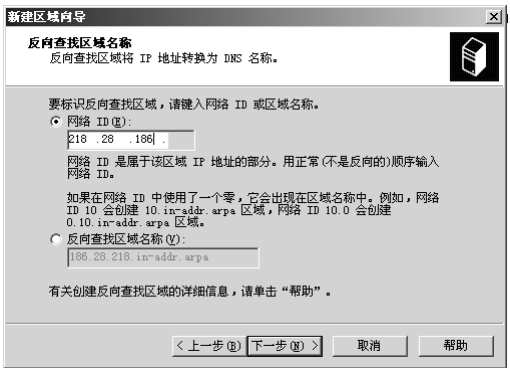

图 4.18　建立反查找区域名称

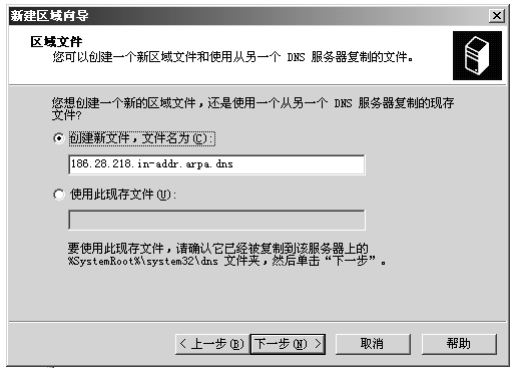

图 4.19　创建反向查找区域文件

（6）在打开的“动态更新”向导页中，指定该 DNS 区域能够接收的注册信息更新类型。允许动态更新可以让系统自动地在 DNS 中注册有关信息，因此选择“允许非安全和安全动态更新”单选框，单击“下一步”按钮，如图 4.20 所示。

（7）最后单击“完成”按钮结束创建。

【实验五】 创建域名的 PTR（枚举指针 DNS 记录）

反向查找区域即是这里所说的 IP 反向解析，它的作用是通过查询 IP 地址的 PTR 记录来得到该 IP 地址指向的域名，当然，要成功得到域名就必须要有该 IP 地址的 PTR 记录。

【实验步骤】

（1）选择“开始”→“管理工具”→“DNS”菜单命令，打开“dnsmgmt”控制台窗口。

（2）在左窗格中依次展开“FLYING-X”→“反向查找区域”目录。然后右键单击“218.28.186.x.Subnet”区域，执行快捷菜单中的“新建指针（PTR）”命令，如图 4.21 所示。

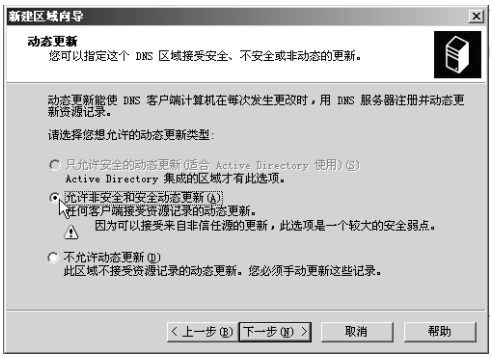

图 4.20　确定动态更新类型图

图 4.21　执行新建主机命令

（3）打开“新建资源记录”对话框，在“主机 IP 号”编辑框中输入“www.hncc.net“域名对应的 IP 地址。在“主机名”编辑框中输入“www.hncc.net“域名对应的 IP 地址，单击“确定”按钮，如图 4.22 所示。

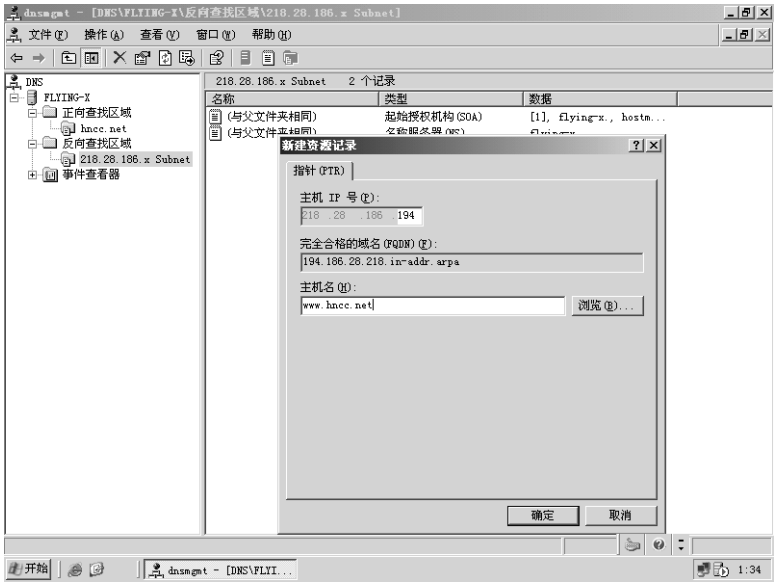

图 4.22　创建枚举指针 DNS 记录

【实验六】 DNS 客户端配置

尽管 DNS 服务器已经创建成功，并且创建了合适的域名，可是如果在客户机的浏览器中

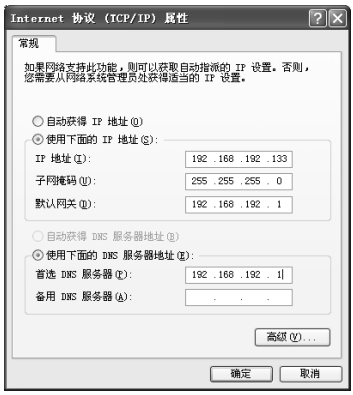

图 4.23　设置客户端 DNS 服务器地址

无法使用“www.hncc.net”这样的域名访问网站。这是因为虽然已经有了 DNS 服务器，但客户机并不知道 DNS 服务器在哪里，因此不能识别用户输入的域名。用户必须手动设置 DNS 服务器的 IP 地址才行。

【实验步骤】

（1）Windows 平台

选择“开始”→“设置”→“网络和拨号连接”命令，并右键单击“本地连接”，然后从弹出的快捷菜单中选择“属性”→“Internet 协议（TCP/IP）”→“属性”对话框中的“首选 DNS 服务器”编辑框中设置刚刚部署的 DNS 服务器的 IP 地址（本例为 192.168.192.1），如图 4.23 所示。

（2）类 UNIX 平台

```
vi /etc/resolv.conf
```

#修改 resolv.conf 内容为以下。

```
nameserver 202.102.224.68
nameserver 202/102/227/68
```

【实验七】 测试 DNS 服务器

【实验步骤】

在 Windows 2000/2003/XP 中，选择“开始”→“运行”→“输入‘CMD’”→“Enter”→“输入‘ipconfig　/all’”，然后按“Enter”键，如果 DHCP 服务器运行正常，可以得到如下信息。

```
C:\Documents and Settings\Administrator>nslookup
Default Server: ns1.hazzptt.net.cn
Address: 192.168.192.1
> www.hncc.net
Server: 192.168.192.1
Address: 202.102.224.68
DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
Name: www.hncc.net
Address: 218.28.184.194
> 218.28.184.194
Server: 192.168.192.1
Address: 202.102.224.68
Name: www.hncc.net
Address: 218.28.184.194
```

任务二　Red Hat Enterprise Linux 5 部署 DNS 服务

4.2.1　任务目的

本任务的目的在于掌握 Red Hat Enterprise Linux 5 DNS 服务的安装和设置方法。

4.2.2　实现参考

实验环境

Red Hat Linux 企业版 5.4

【实验一】 安装 Red Hat 企业版 5 DNS 服务组件 BIND 9

BIND 是一种开源的 DNS（Domain Name System）协议的实现，包含对域名的查询和响应所需的所有软件。它是互联网上最广泛使用的一种 DNS 服务器，对于类 UNIX 系统来说，已经成为事实上的标准。

【实验步骤】

（1）通过本地光盘安装 BIND 9 及相关软件包

① 把 Red Hat Linux 企业版 5.4 的安装 DVD 光盘放入计算机的光驱。

② 在文本命令行界面下建立光驱的挂载点，并挂载光驱。

```
mkdir /mnt/cdrom
mount -t iso9660 /dev/cdrom /mnt/cdrom/
```

③ 进入 Red Hat Linux 企业版 5 的安装 DVD 光盘的软件包目录。

```
cd /mnt/cdrom/CentOS/
```

④ 安装 BIND 9 及相关软件包

```
 rpm -ivh bind-devel-9.3.6-4.P1.el5.i386.rpm
 rpm -ivh bind-libs-9.3.6-4.P1.el5.i386.rpm
 rpm -ivh bind-utils-9.3.6-4.P1.el5.i386.rpm
 rpm -ivh bind-9.3.6-4.P1.el5.i386.rpm
 rpm -ivh bind-chroot-9.3.6-4.P1.el5.i386.rpm
[root@centos CentOS]#rpm -ivh caching-nameserver-9.3.6-4.P1.el5.i386.rpm
```

⑤ 检测 BIND 9 组件的安装情况。

```
rpm -qa bind*
```

显示以下结果：

```
bind-9.3.6-4.P1.el5
```

```
bind-libs-9.3.6-4.P1.el5
bind-chroot-9.3.6-4.P1.el5
bind-utils-9.3.6-4.P1.el5
bind-devel-9.3.6-4.P1.el5
```

（2）通过网络安装 BIND 9

备注：要确保本机能正常访问 Internet。

```
yum update
yum -y install bind* caching-nameserver
```

【实验二】 修改 BIND 9 的主配置文件、启动 DNS 服务、测试 DNS

【实验步骤】

（1）构建并修改 named.conf

```
① cd /var/named/chroot/etc/
② cp –p named.caching-nameserver.conf named.conf
③ cp –p named.rfc1912.zones named.rfc1912.zones.bak
```

备注：cp 参数-p 除复制源文件的内容外，还将把其修改时间和访问权限也复制到新文件中。这里大多数配置文件的属主是 root，组为 named，如果只是 cp，启动 named 服务时会报错。

```
④ vi named.conf
//
// named.caching-nameserver.conf
//
// Provided by Red Hat caching-nameserver package to configure the
// ISC BIND named(8) DNS server as a caching only nameserver
// (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// DO NOT EDIT THIS FILE - use system-config-bind or an editor
// to create named.conf - edits to this file will be lost on
// caching-nameserver package upgrade.
//
options {
        listen-on port 53 { any; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
```

```
        memstatistics-file "/var/named/data/named_mem_stats.txt";

        // Those options should be used carefully because they disable port
        // randomization
        // query-source    port 53;
        // query-source-v6 port 53;

        allow-query     { any; };
        allow-query-cache { localhost; };
};
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};
view localhost_resolver {
        match-clients      { any; };
        match-destinations { any; };
        recursion yes;
        include "/etc/named.rfc1912.zones";
};
```

（2）修改 named.rfc1912.zones，在文件中添加如下部分并保存

```
zone "hncc.net" IN {
        type master;
        file "hncc.zone";
        allow-update { none; };
};
zone "186.28.218.in-addr.arpa" IN {
        type master;
        file "218.28.186.arpa";
        allow-update { none; };
};
```

（3）生成 hncc.zone, 218.28.186.arpa 区域文件

备注：在/var/named/chroot/var/named/下

```
① cp -p localdomain.zone hncc.zone
② cp -p named.local 218.28.186.arpa
③ vi hncc.zone
$TTL    86400
```

```
@            IN SOA  hncc.net root (
                                  42            ; serial (d. adams)
                                  3H            ; refresh
                                  15M           ; retry
                                  1W            ; expiry
                                  1D )          ; minimum
             IN NS          hncc.net
www     IN A          218.28.186.194
mail    IN A          218.28.186.195
④vi 218.28.186.arpa
$TTL    86400
@       IN      SOA     dns.hncc.net. root.dns.hncc.net.  (
                                  2010011000 ; Serial
                                  28800      ; Refresh
                                  14400      ; Retry
                                  3600000    ; Expire
                                  86400 )    ; Minimum
        IN      NS      hncc.net.
194     IN      PTR     www.hncc.net.
195     IN      PTR     mail.hncc.net.
```

（4）启动 DNS 服务

① 启动 DNS 服务

```
service named start
```

② 重启 DNS 服务

```
service named restart
```

③ 将 named 加入系统自动服务列表

```
chkconfig named on
```

（5）测试 DNS

```
Nslookup
```

任务三　BIND View 加速多出口网络互访

4.3.1　任务目的

南北方网络互访的问题一直以来就是广大运行维护人员的心病，两大网络运营商之间的连接带宽比较有限，跟不上互联网业务发展的速度。通过 BIND View 功能可以实现快速互访。

4.3.2　任务描述

利用 BIND 的 View 功能实现域名的智能解析。自动根据客户端 IP 来判断，网通电信的用户解析出网通的 IP，中国教育科研计算机网的用户解析出中国教育科研计算机网的 IP。

测试做的域名：www.hncc.edu.cn。

电信、网通用户访问 www.hncc.edu.cn 会解析到 218.28.186.194。

中国教育科研计算机网访问 www.hncc.edu.cn 会解析到 125.219.124.34。

4.3.3　相关基础知识

普通的 DNS 服务器只负责为用户解析出 IP 记录，而不去判断用户从哪里来，这样会造成所有用户都只能解析到固定的 IP 地址上。

智能 DNS 策略解析很好地解决了上面所述的问题。DNS 策略解析最基本的功能是可以智能的判断访问您网站的用户，然后根据不同的访问者把域名分别解析成不同的 IP 地址。如访问者是网通用户，DNS 策略解析服务器会把域名对应的网通 IP 地址解析给这个访问者。如果访问者是电信用户，DNS 策略解析服务器会把域名对应的电信 IP 地址解析给这个访问者。

4.3.4　实现参考

实验环境

安装有 BIND 9 的计算机

【实验一】 配置 BIND 9 实现域名智能解析

实验步骤

备注：本实验为一河南交通职业技术学院校园网实际情况为例：

（1）修改 named.conf。

```
// Red Hat BIND Configuration Tool
//
// Default initial "Caching Only" name server configuration
//
options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        forwarders {
                202.196.64.1;
                202.196.64.2;
        };
        pid-file "/var/run/named/named.pid";
```

```
        allow-query { any; };
        allow-transfer { any; };
        /*
         * If there is a firewall between you and nameservers you want
         * to talk to, you might need to uncomment the query-source
         * directive below.  Previous versions of BIND always asked
         * questions using port 53, but BIND 8.1 uses an unprivileged
         * port by default.
         */
         // query-source address * port 53;
};
#以下 ACL 内容为中国教育科研计算机网络地址
acl "Cernet" {
  125.219.124.0/24;
  125.219.125.0/24;
  125.219.126.0/24;
  125.219.127.0/24;
  172.16.0.0/16;
  192.168.0.0/16;
  58.154.0.0/15;
  58.192.0.0/12;
  59.64.0.0/12;
  110.64.0.0/15;
  111.114.0.0/15;
  111.116.0.0/15;
  111.186.0.0/15;
  113.54.0.0/15;
  114.212.0.0/15;
  114.214.0.0/16;
  115.24.0.0/14;
  115.154.0.0/15;
  115.156.0.0/15;
  115.158.0.0/16;
  116.13.0.0/16;
  116.56.0.0/15;
  118.202.0.0/15;
  118.228.0.0/15;
  118.230.0.0/16;
  120.94.0.0/15;
  121.48.0.0/15;
```

```
    121.52.160.0/19;
    121.192.0.0/14;
    121.248.0.0/14;
    122.204.0.0/14;
    125.216.0.0/13;
    162.105.0.0/16;
    166.111.0.0/16;
    180.84.0.0/15;
    180.201.0.0/16;
    180.208.0.0/15;
    202.4.128.0/19;
    202.38.64.0/18;
    202.38.140.0/23;
    202.38.184.0/21;
    202.38.192.0/18;
    202.112.0.0/13;
    202.120.0.0/15;
    202.127.216.0/21;
    202.127.224.0/19;
    202.179.240.0/20;
    202.192.0.0/12;
    203.91.120.0/21;
    210.25.0.0/17;
    210.25.128.0/18;
    210.26.0.0/15;
    210.28.0.0/14;
    210.32.0.0/12;
    211.64.0.0/13;
    211.80.0.0/13;
    218.192.0.0/13;
    219.216.0.0/13;
    219.224.0.0/13;
    219.242.0.0/15;
    219.244.0.0/14;
    222.16.0.0/12;
    222.192.0.0/12;
};
#当访问者的 IP 地址为中国教育科研计算机网络用户时，使用该文件中的内容对域名进行解析
view "CERNET"
{
```

```
        match-clients         { Cernet; };
        recursion yes;

    zone "." IN {
        type hint;
        file "named.root";
    };

    zone "localdomain." IN {
        type master;
        file "localdomain.zone";
        allow-update { none; };
    };

    zone "localhost." IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
    };

    zone "0.0.127.in-addr.arpa." IN {
        type master;
        file "named.local";
        allow-update { none; };
    };

    zone "hncc.edu.cn." IN {
        type master;
        file "hncc.edu.cn.zone";
        allow-update { none; };
    };

    zone "124.219.125.in-addr.arpa." IN {
        type master;
        file "named.125.219.124";
        allow-update { none; };
    };

    zone
"0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa." IN {
```

```
        type master;
        file "named.ip6.local";
        allow-update { none; };
};

zone "255.in-addr.arpa." IN {
        type master;
        file "named.broadcast";
        allow-update { none; };
};
zone "0.in-addr.arpa." IN {
        type master;
        file "named.zero";
        allow-update { none; };
};
};
#当访问者的 IP 地址为非中国教育科研计算机网络用户时，使用该文件中的内容对域名进行解析
view "Other"
{
        match-clients          { any; };
        recursion no;

zone "." IN {
        type hint;
        file "named.root";
};

zone "localdomain." IN {
        type master;
        file "localdomain.zone";
        allow-update { none; };
};

zone "localhost." IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};

zone "0.0.127.in-addr.arpa." IN {
```

```
        type master;
        file "named.local";
        allow-update { none; };
    };

    zone "hncc.edu.cn." IN {
        type master;
        file "telcom-cnc.hncc.edu.cn.zone";
        allow-update { none; };
    };

    zone  "186.28.218.in-addr.arpa." IN {
        type master;
        file "named.218.28.186";
        allow-update { none; };
    };

    zone   "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.
arpa." IN {
        type master;
        file "named.ip6.local";
        allow-update { none; };
    };

    zone "255.in-addr.arpa." IN {
        type master;
        file "named.broadcast";
        allow-update { none; };
    };

    zone "0.in-addr.arpa." IN {
        type master;
        file "named.zero";
        allow-update { none; };
    };
    };
    include "/etc/rndc.key";
```

（2）构建区域文件，所构建文件都要放置在/var/named/chroot/var/named 文件夹下。构建中国教育科研计算机网用户解析用域文件。

hncc.edu.cn.zone 文件的内容：

```
$TTL    86400
@       IN      SOA    dns.hncc.edu.cn. root.dns.hncc.edu.cn.  (
                                2008111500 ; Serial
                                28800      ; Refresh
                                14400      ; Retry
                                3600000    ; Expire
                                86400 )    ; Minimum
@           IN    NS     dns.hncc.edu.cn.
@           IN    MX 10 mail.hncc.edu.cn.
mail    IN      A       125.219.124.34
ftp     IN      A       125.219.124.35
www     IN      A       125.219.124.36
dns     IN      A       125.219.124.8
named.125.219.124 文件的内容
$TTL    86400
@       IN      SOA    dns.hncc.edu.cn. root.dns.hncc.edu.cn.  (
                                2008111500 ; Serial
                                28800      ; Refresh
                                14400      ; Retry
                                3600000    ; Expire
                                86400 )    ; Minimum
@           IN    NS     dns.hncc.edu.cn.
@           IN    MX 10 mail.hncc.edu.cn.
8       IN      PTR     dns.hncc.edu.cn.
34       IN      PTR     mail.hncc.edu.cn.
35       IN      PTR     ftp.hncc.edu.cn.
36       IN      PTR     www.hncc.edu.cn.
```

构建非中国教育科研计算机网用户解析用域文件。

telcom-cnc.hncc.edu.cn.zone 的内容：

```
$TTL    86400
@       IN      SOA    dns.hncc.edu.cn. root.dns.hncc.edu.cn.  (
                                2008111500 ; Serial
                                28800      ; Refresh
                                14400      ; Retry
                                3600000    ; Expire
                                86400 )    ; Minimum
@           IN    NS     dns.hncc.edu.cn.
@           IN    MX 10 mail.hncc.edu.cn.
```

```
mail    IN      A       218.28.186.195
www     IN      A       218.28.186.194
dns     IN      A       125.219.124.8
rtx     IN      A       218.28.186.199
ftp     IN      A       218.28.186.196
```

named.218.28.186 文件的内容：

```
$TTL    86400
@       IN      SOA    dns.hncc.edu.cn. root.dns.hncc.edu.cn.  (
                                2008111500 ; Serial
                                28800      ; Refresh
                                14400      ; Retry
                                3600000    ; Expire
                                86400 )    ; Minimum
@           IN    NS     dns.hncc.edu.cn.
@           IN    MX 10  mail.hncc.edu.cn.
195       IN     PTR     mail.hncc.edu.cn.
197      IN      PTR     ftp.hncc.edu.cn.
194      IN      PTR     www.hncc.edu.cn.
```

小　结

通过本项目中各任务的实现，掌握 DNS 的基本概念和工作原理，掌握智能 DNS。

思考与拓展

1．分析访问 www.hncc.edu.cn 时 DNS 的解析过程。
2．DNS 控制台不能连接服务器怎么办？
3．DNS 服务器不能正确解析名称怎么办？

项目 5

部署 FTP 服务

学习目标

FTP（File Transfer Protocol）是文件传输协议的简称。用于 Internet 上控制文件的双向传输。同时，它也是一个应用程序（Application）。用户可以通过它把自己的 PC 与世界各地所有运行 FTP 协议的服务器相连，访问服务器上的大量程序和信息。

- 认识 FTP；
- 掌握 Windows 2003 操作系统平台下构建利用 Serv-U 构建 FTP 服务；
- 掌握 Linux 操作系统平台下构建 FTP 服务。

内容框架

项目 5 的内容框架如图 5.1 所示。

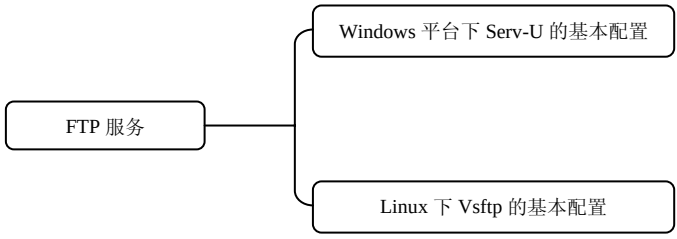

图 5.1　内容框架

任务一　利用 Serv-U 部署 Windows 平台下的 FTP 服务

5.1.1　任务目的

利用 Serv-U 部署 FTP 服务。

5.1.2　任务描述

现在 Windows 平台的用户 90%的 FTP 服务器都是用的 Serv-U 来架设的，Serv-U 从最开

始的版本到现在的 7.x 版本，功能上、界面上都有了很大的变化，安全性也有很大的提高。本小节就以 Serv-U 9.2 版本架设 FTP 服务器。

5.1.3 相关基础知识

FTP（File Transfer Protocol）是文件传输协议的简称。用于 Internet 上控制文件的双向传输。同时，它也是一个应用程序（Application）。用户可以通过它把自己的 PC 与世界各地所有运行 FTP 协议的服务器相连，访问服务器上的大量程序和信息。

与大多数 Internet 服务器一样，FTP 也是一个客户机/服务器系统。用户通过一个支持 FTP 协议的客户机程序，连接到在远程主机上的 FTP 服务器程序。用户通过客户机程序向服务器程序发出命令，服务器程序执行用户所发出的命令，并将执行的结果返回到客户机。比如，用户发出一条命令，要求服务器向用户传送某一份文件的复制，服务器会响应这条命令，将指定文件送至用户的机器上。客户机程序代表用户接收到这个文件，将其存放在用户目录中。

在 FTP 的使用当中，用户经常遇到两个概念“下载（Download）”和“上传（Upload）”。“下载”文件就是从远程主机复制文件至自己的计算机上；“上传”文件就是将文件从自己的计算机中复制至远程主机上。用 Internet 语言来说，用户可通过客户机程序向（从）远程主机上传（下载）文件。

使用 FTP 时必须首先登录，在远程主机上获得相应的权限以后，方可上传或下载文件。也就是说，要想同哪一台计算机传送文件，就必须具有哪一台计算机的适当授权。换言之，除非有用户名和口令，否则便无法传送文件。这种情况违背了 Internet 的开放性，Internet 上的 FTP 主机何止千万，不可能要求每个用户在每一台主机上都拥有账号。匿名 FTP 就是为解决这个问题而产生的。

匿名 FTP 是这样一种机制，用户可通过它连接到远程主机上，并从其下载文件，而无须成为其注册用户。系统管理员建立了一个特殊的用户名，名为 anonymous，Internet 上的任何人在任何地方都可使用该用户名。

5.1.4 实现参考

实验环境

Windows 操作系统平台

【实验一】 安装 Serv-U 9.2

【实验步骤】

（1）双击 Serv-U 的安装程序，选择适合的语言，如图 5.2 所示。

（2）这时会弹出安装的一些信息，直接单击“下一步”按钮，如图 5.3 所示。

（3）许可协议，选择“我接受协议”，单击“下一步”按钮，如图 5.4 所示。

（4）单击“浏览”按钮选择 Serv-U 的安装路径，也可以保持默认值，单击“下一步”按钮，如图 5.5 所示。

（5）在开始程序创建快捷方式，单击“下一步”按钮，如图 5.6 所示。

（6）选择额外任务，根据自己的情况选择，单击“下一步”按钮，如图 5.7 所示。

图 5.2　选择适合的语言

图 5.3　安装信息

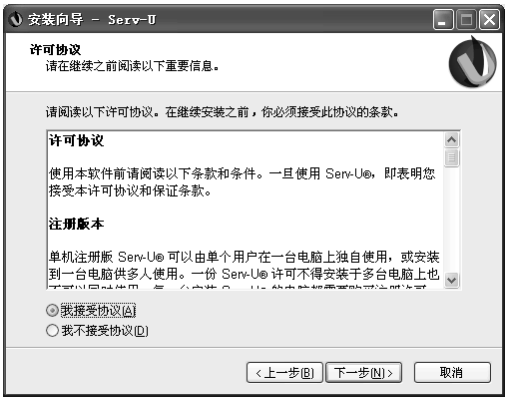

图 5.4　许可协议

图 5.5　选择 Serv-U 的安装路径

图 5.6　开始程序创建快捷方式

图 5.7　选择额外任务

（7）显示 Serv-U 的安装信息。单击“安装”按钮，开始安装 Serv-U，如图 5.8 所示。

（8）安装完成之后，会显示相关产品的信息，单击“关闭”按钮，如图 5.9 所示。

（9）这时 Serv-U 已经安装完了，选择“启动 Serv-U 管理控制台”选项，单击“完成”按钮，开始初始化 FTP 服务器，如图 5.10 所示。

（10）启动 7.2 版本的管理界面，会询问是否定义域，选择“是”，如图 5.11 所示。

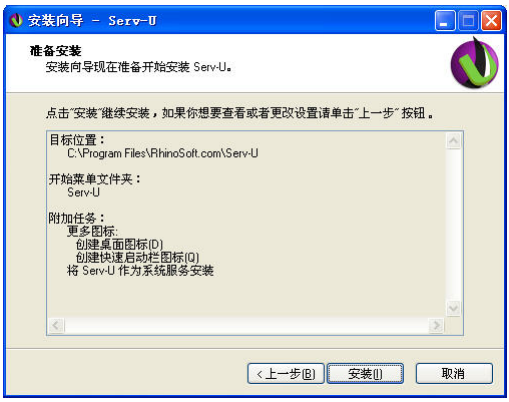

图 5.8　显示 Serv-U 的安装信息

图 5.9　显示 Rhinosoft 公司的相关产品的信息

图 5.10　完成 Serv-U 安装

图 5.11　定义新域

（11）输入域名和域信息，如图 5.12 所示。

（12）根据自己的情况开启服务端口，如图 5.13 所示。

图 5.12　设置新域信息

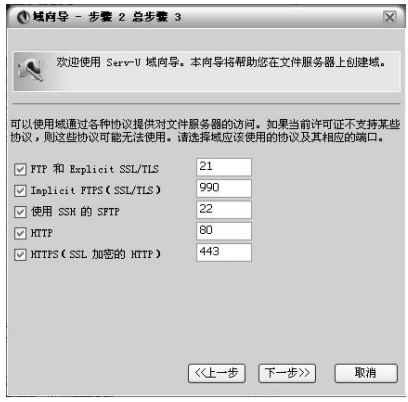

图 5.13　设置服务端口

（13）填写服务器的 IP 地址，如果是动态的就不填，然后单击“完成”按钮，如图 5.14 所示。

（14）到 FTP 服务器便架设完成了，下面再添加一些用户账户就可以了，如图 5.15 所示。

图 5.14　配置服务器域 IP 地址

图 5.15　FTP 服务器安装设置完成

【实验二】 开启 FTP 的匿名访问功能

【实验步骤】

（1）打开管理控制台，打开创建、修改和删除用户，如图 5.16 所示。

图 5.16　Serv-U 管理控制台-用户窗口

（2）单击“添加”按钮，出现如图 5.17 所示对话框，在该对话框中的“登录 ID”处输入“anonymous”，在“根目录”处单击“浏览”按钮，选择该用户的根目录。anonymous 表明建立了一个匿名用户，从客户端登录时不用输入用户名就可以登录。单选框“锁定用户至根目录”和“总是允许登录”、“启用账户”默认是选定的，保持默认状态，“总是允许登录”、“启用账户”一定要选定。“管理权限”可以设定匿名用户的权限。“账户类型”设置账户属于某类型账户。

（3）单击“目录访问”标签，出现如图 5.18 所示对话框。

图 5.17 “用户属性”对话框

图 5.18 用户属性的目录属性标签

（4）单击“添加”按钮，出现如图 5.19 所示对话框，单击“浏览”按钮，选择 anonymous 用户可以访问的目录。

（5）选择可以访问的目录，如图 5.20 所示，选择后单击“选择”按钮，返回到图 5.19 所示的对话框中，然后单击“保存”按钮。

图 5.19 “目录访问规则”对话框

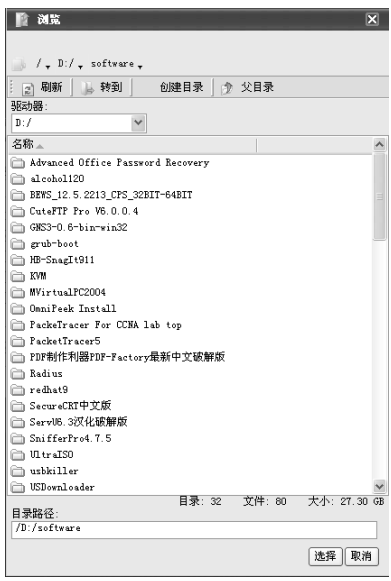

图 5.20 选择目录

【实验三】 添加具有上传功能的账号

【实验步骤】

（1）打开管理控制台，打开创建、修改和删除用户，如图 5.16 所示。

（2）单击“添加”按钮，出现如图 5.17 所示窗口，在该窗口中的“登录 ID”处输入“upload”，“根目录”处单击“浏览”按钮，选择该用户的根目录。

（3）单击“目录访问”标签，出现如图所示 5.18 窗口。

（4）单击“添加”按钮，出现如图 5.19 所示窗口，单击“浏览”按钮，选择“upload”用户可以访问的目录。

（5）选择可访问的目录，如图 5.20 所示，选择后单击“选择”按钮，回到图 5.21 所示窗口中，设置相应的“文件”、“目录”权限，然后单击“保存”按钮。

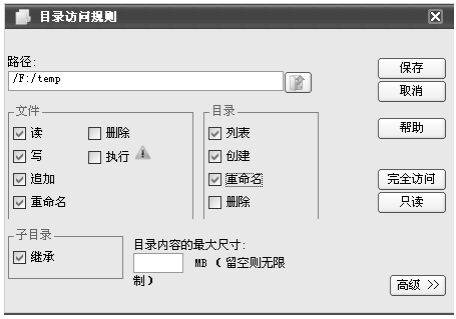

图 5.21　目录访问规则

（6）测试上传功能。

任务二　利用 Vsftp 部署 Linux 平台下的 FTP 服务

5.2.1　任务目的

利用 Vsftp 部署 Linux 平台下的 FTP 服务。

5.2.2　任务描述

Vsftp 是（Very security ftp）的缩写。是 Linux 系统下最常见、最常用的 FTP 服务器架设软件。

5.2.3　相关基础知识

Vsftp 的访问方式。

Vsftp 架设的 FTP 文件服务器，提供 3 种远程的登录方式。

1．匿名登录方式

匿名登录方式就是不需要用户名、密码。就能登录到服务器计算机里面。

2．本地用户方式

本地用户方式是需要用户名和密码才能登录。而且，这个用户名和密码，都是在 Linux 系统里已经有的用户。

3．虚拟用户方式

同样需要用户名和密码才能登录。但是和上面的区别是，这个用户名和密码，在 Linux 系统中是没有的（没有该用户账号）。

5.2.4 实现参考

实验环境

安装 CentOS 5.4 的计算机。

【实验一】 安装、启动 Vsftp

【实验步骤】

（1）把 Red Hat Linux 企业版 5.4 的安装 DVD 光盘放入计算机的光驱。

（2）在文本命令行界面下建立光驱的挂载点，并挂载光驱。

```
mkdir /mnt/cdrom
mount -t iso9660 /dev/cdrom /mnt/cdrom/
```

（3）进入 Red Hat Linux 企业版 5 的安装 DVD 光盘的软件包目录。

```
cd /mnt/cdrom/CentOS/
```

（4）安装 Vsftp。

```
[root@centos CentOS]# rpm -ivh vsftpd-2.0.5-16.el5.i386.rpm
```

或者通过 yum 安装

```
[root@centos CentOS]#yum install vsftpd
```

（5）启动 Vsftp。

```
[root@centos CentOS]# service vsftpd start
```

（6）把 Vsftp 添加到系统自动启动。

```
[root@centos CentOS]#chkconfig --level 2345 vsftpd on
```

（7）测试

在浏览器的地址栏中输入 ftp://ftp 服务器地址（本例中是 172.16.255.2），出现如图 5.22 所示，说明正确运行。

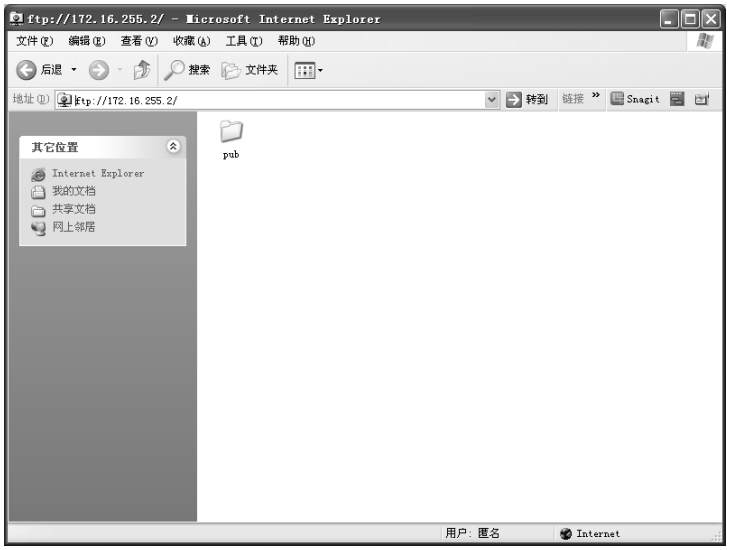

图 5.22　访问 ftp 服务器

【实验二】 配置实现虚拟用户访问

【实验步骤】

（1）修改配置文件。

```
vi /etc/vsftpd/vsftpd.conf
```

要修改的内容如下：

```
listen=yes
anonymous_enable=no
dirmessage_enable=yes
xferlog_enable=yes
xferlog_file=/var/log/vsftpd.log
chroot_local_user=yes
guest_enable=yes
guest_username=virtual
user_config_dir=/etc/vsftpd_user_conf
pam_service_name=vsftpd.vu
local_enable=yes
guest_enable=yes
guest_username=virtual
```

（2）创建虚拟用户列表。

在/etc/vsftpd 文件夹下，创建 loguser.txt 文件

vi /etc/vsftpd/loguser.txt，内容就是准备好的用户名和密码，上行用户名，下行密码。然后再重复，内容如下：

```
username1
```

```
password1
username2
password2
username3
password3
```

（3）安装“db”生成数据库软件包。

虚拟用户模式，是需要 Linux 系统采用“数据库”的方式来保存账号信息的。这里用的是“db”数据库软件包。

```
[root@centos CentOS]# rpm -ivh db4-utils-4.3.29-10.el5.i386.rpm
```

或者

```
[root@centos CentOS]#yum install db*
```

（4）生成数据库。

安装完成后，在/etc/vsftpd 文件夹下输入：

```
[root@centos vsftpd]# db_load -T -t hash -f loguser.txt /etc/vsftpd_login.db
```

（5）设置创建出来的数据库文件的权限。

```
[root@centos vsftpd]# chmod 600 /etc/vsftpd_login.db
```

（6）创建虚拟用户文件夹，有几个虚拟用户就要创建几个文件夹并修改权限。

```
mk /home/ftp/username1
mk /home/ftp/username2
mk /home/ftp/username3
…
…
```

（7）修改文件夹权限。

```
chmod757 username1
chmod757 username2
chmod757 username3
```

（8）为虚拟用户创建一个本地用户。

新建一个系统用户 Virtual，不用设置用户的密码。用户目录为/home/ftp，用户登录终端设置为/bin/false（即使不能登录系统），命令两条：

```
[root@centos vsftpd]#useradd virtual -d /home/ftp -s /bin/false
[root@centos vsftpd]#chown virtual:virtual /home/ftp
```

注意：如果第 2 条命令，说没有找到 Virtual 组，就自己新建这个组。

（9）设置虚拟用户权限，和本地用户模式的方法一样，建/etc/vsftpd/vsftpd_user_conf 文件夹。

```
[root@centos vsftpd]#mkdir /etc/vsftpd/vsftpd_user_conf
```

（10）每个用户都要单独创建，然后在里面写上具体的、单独的，只针对这个用户，他所拥有的权限，比如：

- 创建 username1，username1 有读的权限

```
[root@centos vsftpd]#vi /etc/vsftpd/vsftpd_user_conf/username1
```

文件内容如下：

```
write_enable=YES
local_root=/home/ftp/username1
```

- 创建 username2，username2 有上传、下载和浏览的权限。

```
vi /etc/vsftpd/vsftpd_user_conf/username2
```

文件内容如下：

```
Anon_world_readable_only=no
Write_enable=yes
Anon_upload_enable=yes
local_root=/home/ftp/username2
```

- 创建 username3，username3 有上传、下载、删除文件目录、修改文件名和浏览的权限。

```
vi /etc/vsftpd/vsftpd_user_conf/username3
```

文件内容如下：

```
write_enable=YES
anon_world_readable_only=NO
anon_upload_enable=YES
anon_mkdir_write_enable=YES
anon_other_write_enable=YES
local_root=/home/ftp/username3
```

（11）配置 pam（用于 FTP 对用户的验证），新建/etc/pam.d/vsftpd.vu 文件。

```
vi /etc/pam.d/vsftpd.vu
```

文件内容如下：

```
auth required /lib/security/pam_userdb.so db=/etc/vsftpd_login
account required /lib/security/pam_userdb.so db=/etc/vsftpd_login
```

项目 6

部署 DHCP 服务

学习目标

在使用 TCP/IP 协议的网络中，每台主机都必须有唯一的 IP 地址，并通过该地址与网络中的其他主机进行通信。在网络规模不是很大的情况下，可以用手动的方式给网络中的主机分配 IP 地址。但是，当网络规模很大时，其工作量就很大，对于网络中的 IP 地址也不太容易管理，加重了网络管理的负担，在这种情况下就可以使用 DHCP 服务。

- 认识 DHCP 服务；
- 理解 DHCP 服务的工作原理；
- 掌握 Windows 2003 操作系统平台下部署 DHCP 服务；
- 掌握 Linux 操作系统平台下部署 DHCP 服务。

内容框架

项目 6 的内容框架如图 6.1 所示。

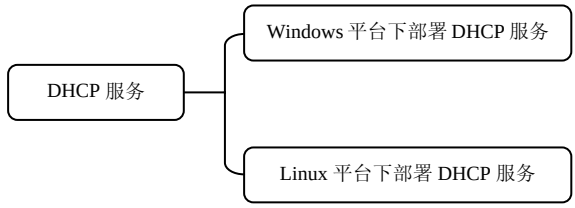

图 6.1　内容框架

任务一　部署 Windows 平台下的 DHCP 服务

6.1.1　任务目的

本任务的目的在于掌握 Windows Server 2003 DHCP 服务的安装和设置方法，从而对 DHCP 的工作原理有一定的认知。

6.1.2　任务描述

在安装了 Windows Server 2003 企业版的计算机上部署 DHCP 服务器。

6.1.3　相关基础知识

DHCP（Dynamic Host Configuration Protocol，动态主机分配协议）的前身是 BOOTP。BOOTP 原本是用于无磁盘主机连接网络上的：网络主机使用 BOOT ROM 而不是磁盘启动并连接上网络，BOOTP 则可以自动地为那些主机设定 TCP/IP 环境。

DHCP 可以说是 BOOTP 的增强版本，它分为两个部分：一个是服务器端，另一个是客户端。所有的 IP 网络设定数据都由 DHCP 服务器集中管理，并负责处理客户端的 DHCP 要求；而客户端则会使用从服务器分配下来的 IP 环境数据。比较起 BOOTP，DHCP 透过“租约”的概念，有效且动态地分配客户端的 TCP/IP 设定，而且，作为兼容考虑，DHCP 也完全照顾了 BOOTP Client 的需求。DHCP 的分配形式：首先，必须至少有一台 DHCP 工作在网络上，它会监听网络的 DHCP 请求，并与客户端搓商 TCP/IP 的设定环境。

DHCP 除了能动态的设定 IP 位址之外，还可以将一些 IP 保留下来给一些特殊用途的机器使用，它可以按照硬体位址来固定的分配 IP 位址，这样可以给您更大的设计空间。同时，DHCP 还可以帮客户端指定 Router、Netmask、DNS Server、WINS Server 等项目，您在客户端上，除了将 DHCP 选项打勾之外，几乎无须做任何的 IP 环境设定。

1．DHCP 的运行方式

（1）永久租用。当 DHCP 客户端向 DHCP 服务器租用到 IP 地址后，这个地址就永远分派给这个 DHCP 客户端使用。

（2）限定租期当。DHCP 客户端向 DHCP 服务器租用到 IP 地址后，暂时以使用这个地址一段时间。如果原 DHCP 客户端之后又需要 IP 地址，它可以向 DHCP 服务器重新租用另一个 IP 地址。

2．DHCP 的工作原理

（1）向 DHCP 服务器索取新的 IP 地址

① 发现阶段（DHCPDISCOVER）。即 DHCP 客户端寻找 DHCP 服务器的阶段。客户端以广播方式发送 DHCPDISCOVER 包，只有 DHCP 服务器才会响应。

② 提供阶段（DHCPOFFER）。即 DHCP 服务器提供 IP 地址的阶段。DHCP 服务器接收到客户端的 DHCPDISCOVER 报文后，从 IP 地址池中选择一个尚未分配的 IP 地址分配给客户端，向该客户端发送包含租借的 IP 地址和其他配置信息的 DHCPOFFER 包。

③ 选择阶段（DHCPREQUEST）。即 DHCP 客户端选择 IP 地址的阶段。如果有多台 DHCP 服务器向该客户端发送 DHCPOFFER 包，客户端从中随机挑选，然后以广播形式向各 DHCP 服务器回应 DHCPREQUEST 包，宣告使用它挑中的 DHCP 服务器提供的地址，并正式请求该 DHCP 服务器分配地址。其他所有发送 DHCPOFFER 包的 DHCP 服务器接收到该数据包后，将释放已经 OFFER（预分配）给客户端的 IP 地址。

如果发送给 DHCP 客户端的 DHCPOFFER 包中包含无效地配置参数，客户端会向服务器

发送 DHCPCLINE 包拒绝接收已经分配的配置信息。

④ 确认阶段（DHCPACK）。即 DHCP 服务器确认 IP 地址的阶段。当 DHCP 服务器接收到 DHCP 客户端回答的 DHCPREQUEST 包后，便向客户端发送包含它所提供的 IP 地址及其他配置信息的 DHCPACK 确认包。然后，DHCP 客户端将接收并使用 IP 地址及其他 TCP/IP 配置参数。

（2）更新 IP 地址的租约：DHCP 服务器分配给客户端的动态 IP 地址通常有一定的租借期限，期满后服务器会收回该 IP 地址。如果 DHCP 客户端希望继续使用该地址，需要更新 IP 租约。实际使用中，在 IP 地址租约期限达到一半时，DHCP 客户端会自动向 DHCP 服务器发送 DHCPREQUEST 包，以完成 IP 租约的更新。如果此 IP 地址有效，则 DHCP 服务器回应 DHCPACK 包，通知 DHCP 客户端已经获得新 IP 租约。

如果 DHCP 客户端续租地址时发送的 DHCPREQUEST 包中的 IP 地址与 DHCP 服务器当前分配给它的 IP 地址（仍在租期内）不一致，DHCP 服务器将发送 DHCPNAK 消息给 DHCP 客户端。

（3）DHCP/BOOTP 中继代理。DHCP 客户机通过网络广播消息获得 DHCP 服务器的响应后得到 IP 地址。但广播消息是不能跨越子网的。因此，如果 DHCP 客户机和服务器在不同的子网内，客户机还能不能向服务器申请 IP 地址呢？这就要用到 DHCP 中继代理。

绝大部分网络内的 IP 路由器不能将广播信息传递到不同的网络区域内，因此，限制了 DHCP 有效地使用范围。但是只要 IP 路由器具备 DHCP/BOOTP 中继代理的功能，就可以将 DHCP 信息转送到其他的网络区域，如图 6.2 所示。

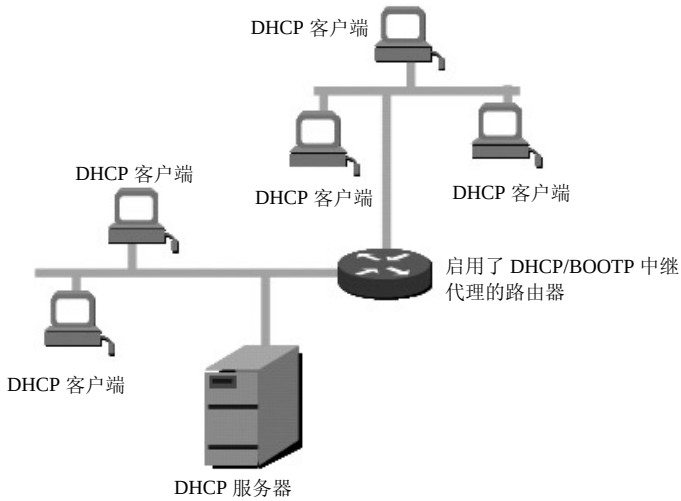

图 6.2　DHCP/BOOTP 中继代理

6.1.4　实现参考

实验环境

Windows Server 2003 企业版。

【实验一】 安装 Windows 2003 企业版 DHCP 网络服务组件

【实验步骤】

DHCP 服务器本身的 IP 地址必须是静态固定的，其 IP 地址、子网掩码、默认网关等数据必须用手动的方式输入。

① 通过选择任务栏的“开始”→“程序”→“管理工具”→“管理您的服务器”命令，启动服务配置窗口，如图 6.3 所示。

图 6.3　启动服务配置

② 在“管理您的服务器”窗口中单击“添加或删除角色”按钮，配置服务器角色，如图 6.4 所示。

图 6.4　管理您的服务器

③ 开启“配置您的服务器向导”对话框后直接单击“下一步”按钮，如图 6.5 所示。

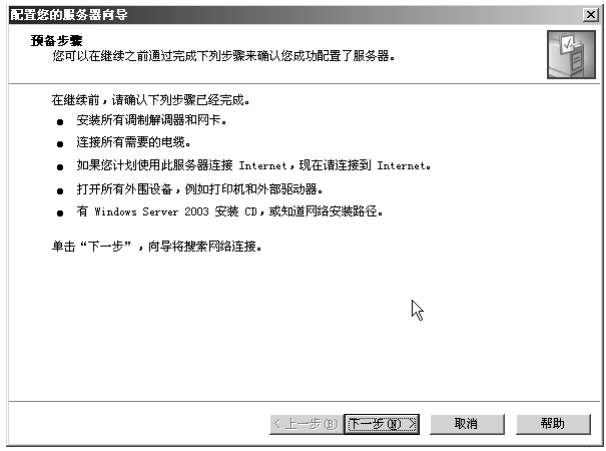

图 6.5 “配置您的服务器向导”对话框

④ 系统会自动扫描当前开启的服务及状态，根据服务器硬件配置所需时间会不同，一般为两分钟左右，如图 6.6 所示。

图 6.6 扫描当前开启的服务及状态

⑤ 如果本机没有开启 DHCP 服务的话，则会在服务器角色中显示 DHCP 服务器已配置状态为“否”，如图 6.7 所示。

⑥ 在图 6.7 所示窗口中选中“DHCP 服务器”然后单击“下一步”按钮，便开始安装 DHCP 服务器，并会自动建立一个新的作用域，如图 6.8 所示。

⑦ 系统配置 DHCP 服务组件，并自动安装到本地计算机的硬盘中，如图 6.9 所示。

【实验二】 配置 DHCP 作用域

【实验步骤】

（1）当组件安装完毕后系统会自动启用“新建作用域向导”，让用户建立一个新的作用域，单击“下一步”按钮，如图 6.10 所示。

图 6.7　DHCP 服务器配置状态

图 6.8　DHCP 服务器安装选择总结

图 6.9　安装 DHCP 服务器过程

图 6.10　新建作用域向导

（2）为建立的作用域起一个名字，单击“下一步”按钮，如图 6.11 所示。

图 6.11　填写作用域名称

（3）配置作用域的 IP 地址范围，设置起始 IP 地址和结束 IP 地址，以及子网掩码的长度及设置。我们可以在子网掩码设置长度处输入数字来快速定位子网掩码的参数。这里设置 DHCP 作用域的 IP 地址为 192.168.192.3 到 192.168.192.252，单击“下一步”按钮，如图 6.12 所示。

（4）接着设置排除的 IP 地址信息，因为在实际使用中很可能一个网段中并不是所有 IP 地址都需要通过自动获得 IP 的方式获得，很多服务需要独立设置 IP 才能工作。所以对于大部分提供服务的客户机都不能通过自动获得 IP 来设置网络参数，所以应该在“添加排除”窗口中将这些 IP 地址排除出去，单击“下一步”按钮，如图 6.13 所示。

（5）设置 IP 地址获得的租约期限，默认为 8 天。可以根据实际情况增加或缩短，单击“下一步”按钮，如图 6.14 所示。

图 6.12　配置作用域的 IP 地址范围

图 6.13　设置排除的 IP 地址信息

图 6.14　设置 IP 地址获得的租约期限

（6）至此就设置完 IP 地址及子网掩码信息了，对于 DNS 及 WINS 等参数属于高级配置。如果希望配置这些信息需要在配置 DHCP 选项步骤中单击“是，我想现在配置这些选项”选项，同理不想配置就单击“否，我想稍后配置这些选项”选项，然后单击“下一步”按钮，如图 6.15 所示。

图 6.15　配置 DHCP 选项

（7）设置路由器地址（即默认网关地址），在 Windows Server 2003 中叫做路由器地址，其实如果网关使用的是代理服务器这里设置的应该是代理服务器的地址。在 IP 地址处输入数值单击“添加”按钮即可，输入 192.168.192.1，单击“下一步”按钮，如图 6.16 所示。

图 6.16　配置 DHCP 选项的默认网关

（8）设置 DNS 和域名称，对于没有加入域的用户来说直接在 IP 地址处输入客户机需要设置的 DNS 地址即可，单击“下一步”按钮，如图 6.17 所示。

图 6.17　配置 DHCP 选项的域名和域名服务器地址

（9）设置 WINS 服务器地址，虽然 WINS 服务器在目前已经很少用了，不过一般情况下还是要配置该参数，设置好 IP 地址后单击“添加”按钮即可，单击“下一步”按钮，如图 6.18 所示。

图 6.18　配置 DHCP 选项的 WINS 服务器地址

（10）最后要激活该作用域才能开始正常工作，选择“是，我想现在激活此作用域”选项，并单击“下一步”按钮，如图 6.19 所示。

（11）完成新建作用域向导全部步骤，如图 6.20 所示。

（12）在配置服务器向导中会出现“此服务器现在是 DHCP 服务器”的提示，如图 6.21 所示。

图 6.19　激活 DHCP 作用域

图 6.20　完成新建作用域

图 6.21　完成 DHCP 服务器配置

（13）选择任务栏的“开始”→“程序”→“管理工具”→“管理您的服务器”命令，查看服务器角色就会发现 DHCP 服务器的配置变成了“是”。这说明配置 DHCP 服务已经成功，如图 6.22 所示。

图 6.22　配置成功后的 DHCP 服务器

DHCP 服务器常常存在于中型及大型网络中，通过它可以大大减少网络管理员维护网络信息的工作量，也使故障排除的难度大大降低。

【实验三】 管理 DHCP 服务器

选择“开始”→“设置”→“控制面板”命令，单击“管理工具”命令，再单击“DHCP”，打开 DHCP 服务管理器。

（1）单击控制台树中适用的 DHCP 服务器。在快捷菜单上指向“所有任务”，然后单击以下任意一选项：

① 启动服务，单击“开始”按钮。

② 停止服务，单击“停止”按钮。

③ 中断服务，单击“暂停”按钮。

④ 停止然后自动重新启动服务，单击“重新启动”按钮，如图 6.23 所示。

图 6.23　管理 DHCP 服务器

在暂停或停止服务器之后，会出现“继续”选项，可以通过单击该选项来立即恢复服务。

也可以在命令提示符下使用下列命令来执行上述任务：

① net start dhcpserver

② net stop dhcpserver

③ net pause dhcpserver

④ net continue dhcpserver

（2）管理 IP 作用域：选择“开始”→“设置”→“控制面板”命令，单击“管理工具”，再单击“DHCP”，打开 DHCP 服务管理器。单击控制台树中适用的 DHCP 服务器。

① 在快捷菜单上单击“新建作用域”复选框，按照“新建作用域向导”中的指示操作。

② 在快捷菜单上单击“删除”按钮，出现提示时，单击“是”删除作用域，如图 6.24 所示。

图 6.24　新建与删除作用域

③ 在快捷菜单上单击“属性”，可以改变 IP 地址范围、租约、DNS 更新、BOOTP 等，如图 6.25 所示。

图 6.25　改变 IP 地址范围、租约、DNS 更新、BOOTP

④ 在“地址池“快捷菜单上单击“新建排除范围”。在“添加排除”对话框中，输入要从该作用域中排除的起始 IP 地址。要排除有多个 IP 地址的范围，请输入结束 IP 地址。单击“添加”按钮，如图 6.26 所示。

图 6.26　新建排除范围

⑤ 在“保留”快捷菜单上单击“新建保留”，可以把某个 IP 地址指定分配给某个主机，如图 6.27 所示。“保留名称”是给保留起个名字，最好是能体现这个保留 IP 的作用的名字。“IP 地址”是保留分配的 IP 地址。“MAC 地址”是被保留 IP 地址的那台主机的物理地址，可通过本地连接查询。这个主机每次需要 IP 地址时，DHCP 服务器都会把这个地址分配给这台主机，一般用于给比较重要的服务器等分配 IP 地址用。

图 6.27　新建保留

【实验四】 DHCP 客户端配置

（1）配置 Windows 客户端

选择“开始”→“设置”→“网络和拨号连接”选项，并右键单击“本地连接”，然后从弹出的快捷菜单中选择“属性”→“Internet 协议（TCP/IP）”→“属性”→“自动获得 IP 地

址”命令，将该计算机设为 DHCP 客户端，如图 6.28 所示。

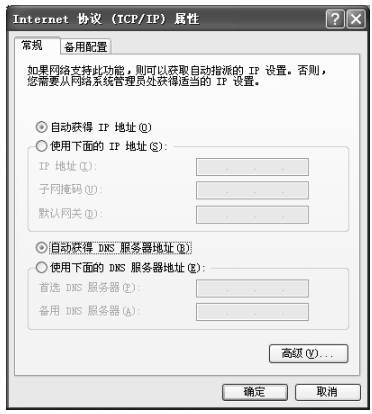

图 6.28　设置 DHCP 客户端

（2）在 Windows 客户端测试 DHCP 服务

在 Windows 2000/2003/XP 中，选择“开始”→“运行”→“输入‘CMD’”→“Enter”→“输入‘ipconfig /all’”，然后按“Enter”键，如果 DHCP 服务器运行正常，可以得到如下信息：

```
C:\Documents and Settings\Administrator>ipconfig /all
Windows IP Configuration
        Host Name . . . . . . . . . . . . : 0FB444E4C8CA4C8
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : Yes
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : hncc.net
Ethernet adapter 本地连接:
        Connection-specific DNS Suffix  . : hncc.net
        Description . . . . . . . . . . . : Realtek RTL8139/810x Family Fast
Ethernet NIC
        Physical Address. . . . . . . . . : 50-76.10-27-49-63
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.166.192.196
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.166.192.1
        DHCP Server . . . . . . . . . . . : 192.166.192.5
        DNS Servers . . . . . . . . . . . : 202.102.224.68
                                    202.102.227.68
        Lease Obtained. . . . . . . . . . : 2008 年 9 月 23 日 10:50:21
        Lease Expires . . . . . . . . . . : 2008 年 9 月 24 日 22:50:21
```

（3）配置 Linux 客户端

```
[root@centos ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0
文件内容如下：
DEVICE=eth0
BOOTPROTO=dhcp
HWADDR=00:0C:29:43:F4:62
ONBOOT=yes
TYPE=Ethernet
USERCTL=no
IPV6INIT=no
PEERDNS=yes
```

（4）在 Linux 客户端测试 DHCP 服务

```
[root@centos ~]# ifconfig
```

任务二　部署 Linux 平台下的 DHCP 服务

6.2.1　任务目的

本任务的目的在于掌握 CentOS 5.4 DHCP 服务的安装和设置方法。

6.2.2　任务描述

在安装了 CentOS 5.4 的计算机上部署 DHCP 服务器。

6.2.3　实现参考

实验环境

CentOS 5.4　企业版。

【实验一】 在 CentOS5.4 上部署 DHCP 服务

（1）安装 DHCP 服务器组件

```
[root@centos CentOS]# rpm -ivh dhcp-3.0.5-21.el5.i386.rpm
[root@centos CentOS]# rpm -ivh dhcp-devel-3.0.5-21.el5.i386.rpm
```

或者

```
[root@centos CentOS]#yum -y install dhcp
```

（2）配置 DHCP

DHCP 配置文件为/etc/dhcpd.conf，但该文件默认是没有内容的，可以从 DHCP 安装目录复制一个到/etc 下。

```
    [root@centos]#cp
/usr/share/doc/dhcp-3.0.5/dhcpd.conf.sample/etc/dhcpd.conf
    [root@centos]#vi /etc/dhcpd.conf
```

文件内容如下：

```
    ddns-update-style none;       #不要更新 DDNS 的设置
    subnet 172.16.255.0 netmask 255.255.255.0 {
    option routers 172.16.255.254;          #网关
    option subnet-mask 255.255.255.0;       #子网掩码
    option domain-name “hncc.edu.cn";       #域名
    option domain-name-servers 202.102.224.68,202.102.227.68; #域名服务器地址
    range 172.16.255.10 172.16.255.253;     #提供的 IP 地址段
    default-lease-time 21600;               #默认租期
    max-lease-time 43200;                   #最大租期
    }
```

（3）因为服务器上有多张网卡所以要指定一下监听设备为 eth0，编辑/etc/sysconfig/dhcpd 文件内容为：

```
    DHCPDARGS=eth0
```

（4）启动 DHCP 服务器

```
    [root@centos]#service dhcpd start
```

（5）让 DHCP 服务随系统而启动：

```
    [root@centos]#chkconfig dhcpd on
```

项目 7

电子邮件服务器的应用

学习目标

电子邮件又称电子信箱，它是一种用电子手段提供信息交换的通信方式。是 Internet 应用最广的服务，通过网络的电子邮件系统，用户可以用非常低廉的价格，以非常快速的方式，与世界上任何一个角落的网络用户联系，这些电子邮件可以是文字、图像、声音等各种方式。同时，用户可以得到大量免费的新闻、专题邮件，并实现轻松的信息搜索。

- 认识 Mail；
- 理解 Mail 的工作原理；
- 掌握 Windows 2003 操作系统平台下部署 Mail 服务。

内容框架

项目 7 的内容框架如图 7.1 所示。

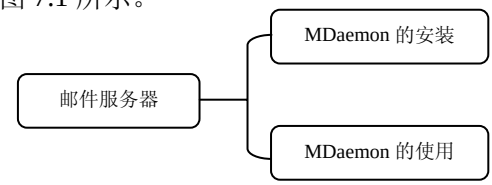

图 7.1　内容框架

任务一　利用 MDaemon 部署 Windows 平台下的 Mail 服务

7.1.1　任务目的

本任务的目的在于掌握 Windows Server 2003 平台 Mail 服务的安装和设置方法，从而对 Mail 的工作原理有一定的认知。

7.1.2　任务描述

在安装了 Windows Server 2003 企业版的计算机上部署 Mail 服务器。

7.1.3 相关基础知识

电子邮件的工作过程遵循客户-服务器模式。每份电子邮件的发送都要涉及发送方与接收方，发送方构成客户端，而接收方构成服务器，服务器含有众多用户的电子信箱。发送方通过邮件客户程序，将编辑好的电子邮件向邮局服务器（SMTP 服务器）发送。邮局服务器识别接收者的地址，并向管理该地址的邮件服务器（POP3 服务器）发送消息。邮件服务器只将消息存放在接收者的电子信箱内，并告知接收者有新邮件到来。接收者通过邮件客户程序连接到服务器后，就会看到服务器的通知，进而打开自己的电子信箱来查收邮件。

通常 Internet 上的个人用户不能直接接收电子邮件，而是通过申请 ISP 主机的一个电子信箱，由 ISP 主机负责电子邮件的接收。一旦有用户的电子邮件到来，ISP 主机就将邮件移到用户的电子信箱内，并通知用户有新邮件。因此，当发送一条电子邮件给另一个客户时，电子邮件首先从用户计算机发送到 ISP 主机，再到 Internet，再到收件人的 ISP 主机，最后到收件人的个人计算机。

ISP 主机起着“邮局”的作用，管理着众多用户的电子信箱。每个用户的电子信箱实际上就是用户所申请的账号名。每个用户的电子邮件信箱都要占用 ISP 主机一定容量的硬盘空间，由于这一空间是有限的，因此用户要定期查收和阅读电子信箱中的邮件，以便腾出空间来接收新的邮件。

MDaemon 是一款著名的标准 SMTP/POP/IMAP 邮件服务系统，由美国 Alt-N 公司开发。它提供完整的邮件服务器功能，保护用户不受垃圾邮件的干扰，实现网页登录收发邮件，支持远程管理，并且当与 MDaemon AntiVirus 插件结合使用时，它还保护系统防御邮件病毒。它安全、可靠、功能强大，是世界上成千上万的公司广泛使用的邮件服务器。

7.1.4 实现参考

实验环境

Windows Server 2003 企业版。

【实验一】 安装 MDaemon

【实验步骤】

（1）双击 MDaemon 的安装程序，出现 MDaemon 的欢迎窗口，如图 7.2 所示，单击“下一步”按钮。

（2）在软件许可协议对话框，单击“我同意”按钮，如图 7.3 所示。

图 7.2 MDaemon 欢迎窗口

图 7.3 软件许可协议

（3）单击“浏览”按钮，将显示选择 MDaemon 安装路径的安装向导，可进行新的安装路径的选择，在该安装路径下，将存放所有用户的邮件。因此建议将 MDaemon 安装到一个剩余磁盘空间大的分区内。然后在选择安装目录对话框中，单击“下一步”按钮，如图 7.4 所示。

（4）填写授权信息的安装向导对话框，在这里可以分别输入用户和单位名称，如图 7.5 所示。

图 7.4　选择安装目录

图 7.5　注册信息

（5）单击“下一步”按钮，将显示“准备安装”对话框，提示用户即将正式安装 MDaemon，如图 7.6 所示。

（6）单击“下一步”按钮，安装进程开始复制文件，以进行 MDaemon 的正式安装。

（7）设置域名，然后单击“下一步”按钮，如图 7.7 所示。

图 7.6　准备安装 MDaemon

图 7.7　设置域名

（8）设置第一个账号，如图 7.8 所示。

（9）在安装完毕后，将显示配置 DNS 对话框，在这里要求输入主 DNS 服务器及备份 DNS 的 IP 地址，如图 7.9 所示。

图 7.8　设置账号

图 7.9　设置 DNS

（10）设置操作模式，然后单击“下一步”按钮，如图 7.10 所示。

（11）设置 MDaemon 的启动模式，然后单击“下一步”按钮，如图 7.11 所示。

图 7.10　设置操作模式

图 7.11　设置启动模式

（12）单击“完成”按钮以完成安装过程，同时并开启管理窗口的主界面，如图 7.12 所示。

【实验二】 MDaemon 中 Web 邮件的实现

【实验步骤】

（1）启动 MDaemon 管理窗口，如图 7.13 所示。

图 7.12　安装完成

图 7.13　MDaemon 控制台

（2）单击“设置”按钮，选择“WorldClient（Web 邮件），如图 7.14 所示。

（3）更改 MDaemon Web 服务的端口，如图 7.15 所示。

图 7.14　设置菜单

图 7.15　更改 MDaemon Web 服务的端口

（4）开启 MDaemon Web 在线申请功能，如图 7.16 所示。

（5）测试 Web Mail，如图 7.17 所示。

图 7.16　开启 MDaemon Web 在线申请功能

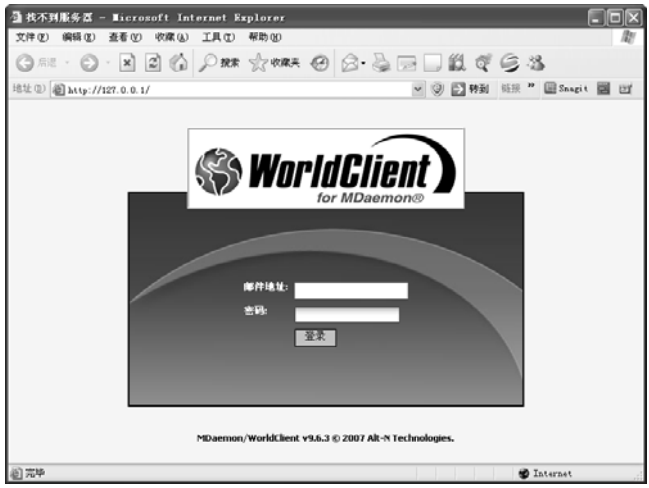

图 7.17　测试 Web Mail

项目 8

让局域网访问互联网

学习目标

局域网是工作应用中的一个重要方面，它能够提供访问互联网服务，这是目前几乎所有局域网必须具备的功能。本项目通过若干任务达到如下目标：

- 掌握通过硬件实现访问互联网。
- 掌握采用软件实现访问互联网。

内容框架

项目 8 的内容框架如图 8.1 所示。

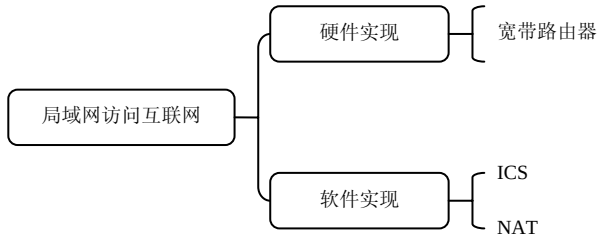

图 8.1　内容框架

任务一　硬件实现访问互联网

8.1.1　任务目的

本任务的目的在于掌握利用宽带路由器实现局域网内计算机访问互联网。

8.1.2　任务描述

利用一个宽带路由器，让局域网内所有计算机都可以访问互联网。

8.1.3　相关基础知识

1．网络结构

无论采用硬件或者软件实现共享上网，通常情况下其网络结构都是一致的，如图 8.2 所示。

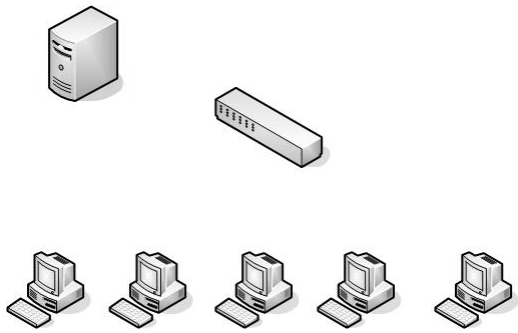

图 8.2　网络出口设备

图中“网络出口设备”即为软件（所在服务器）或硬件（路由器）安装的位置，该设备通常具备两个以太网端口，一是连接局域网，二是用于连接互联网。

2．宽带路由器介绍

宽带路由器是近几年来新兴的一种网络产品，它伴随着宽带的普及应运而生。宽带路由器在一个紧凑的箱子中集成了路由器、防火墙、带宽控制和管理等功能，具备快速转发能力、灵活的网络管理和丰富的网络状态等特点。多数宽带路由器针对中国宽带应用优化设计，可满足不同的网络流量环境，具备良好的电网适应性和网络兼容性。多数宽带路由器采用高度集成设计，集成 10/100Mbps 宽带以太网 WAN 接口，并内置多口 10/100Mbps 自适应交换机，以方便多台机器连接内部网络与 Internet，可以广泛应用于家庭、学校、办公室、网吧、小区接入、政府及企业等场合。

宽带路由器有高、中、低档次之分，高档次企业级宽带路由器的价格可达数千，而目前的低价宽带路由器已降到百元内，其性能已基本能满足像家庭、学校宿舍、办公室等应用环境的需求，已成为组网首选产品之一。

8.1.4　实现参考

【实验一】 宽带路由器共享上网

某办公室目前拥有一个独立的小型局域网，现该单位分配给这个办公室一个互联网出口，其出口的 TCP/IP 协议配置是 IP 地址为 172.16.10.8，子网掩码为 255.255.255.224，网关为 172.16.10.1。应如何做才能实现办公室所有的计算机都能够访问互联网。

【实验步骤】

（1）该项目属于较为简单的局域网共享访问互联网的情况，建议采用宽带路由器的方法解决。网络结构如图 8.3 所示。

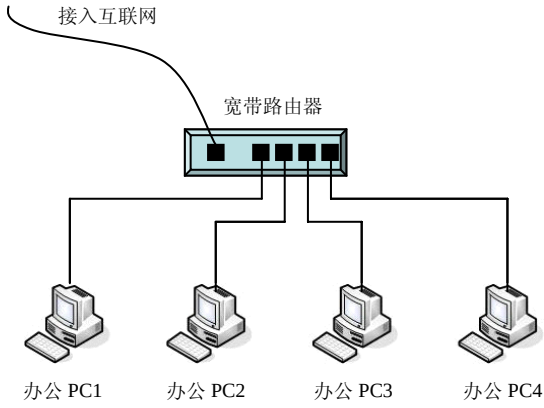

图 8.3　网络结构

（2）配置方法

① 宽带路由器配置。宽带路由器一般有一个 Internet 以太网接口（标记 WAN）和 4 个局域网以太网接口，WAN 端口用于连接 Internet 专线，4 个局域网端口用于连接办公计算机。新购买的宽带路由器默认的局域网地址为 192.16.1.1，使用一台计算机（如办公计算机）将其 IP 地址配置为 192.168.1.2 后，启动 IE 浏览器，在地址栏中输入 http://192.168.1.1 后，即可启动宽带路由器的 Web 管理界面，输入默认的用户名和密码（一般默认为 Admin）后，即可配置宽带路由器。

② 办公局域网配置。办公局域网计算机配置 IP 地址为 192.168.1.X/255.255.255.0，网关配置为 192.168.1.1，并配置相应的 DNS1 与 DNS2。

【总结】

因为宽带路由器已经内置了路由软件，只要保证 WAN 端口能够正常访问 Internet 且局域网地址配置无误，即可实现办公室所有的计算机都能够访问互联网。

思考：

1．简述路由器常用的几种配置方式。

2．观察路由器的基本结构，描述路由器的各种接口及其表示方法。

任务二　利用软件实现共享上网

8.2.1　任务目的

本任务的目的在于掌握利用 ICS 或 NAT 实现局域网内计算机访问互联网。

8.2.2　任务描述

利用 Windows Server 2003 自带的 ICS 或 NAT 功能，让局域网内所有计算机都可以访问互联网。

8.2.3　相关基础知识

1．ICS

ICS（Internet Connection Sharing）是 Windows 2003 针对家庭网络或小型的 Intranet 提供的一种 Internet 连接共享服务。ICS 实际上相当于一种网络地址转换器，所谓网络地址转换器就是当数据包向前传递的过程中，可以转换数据包中的 IP 地址和 TCP/UCP 端口等地址信息。有了网络地址转换器，家庭网络或小型的办公网络中的计算机就可以使用专有地址，并且通过网络地址转换器将专有地址转换成 ISP 分配的单一的公共 IP 地址。

2．NAT

NAT——网络地址转换，是通过将专用网络地址（如企业内部网 Intranet）转换为公用地址（如互联网），从而对外隐藏了内部管理的 IP 地址。这样，通过在内部使用非注册的 IP 地址，并将它们转换为一小部分外部注册的 IP 地址，从而减少了 IP 地址注册的费用及节省了目前越来越缺乏的地址空间（即 IPv4）。同时，也隐藏了内部网络结构，从而降低了内部网络受到攻击的风险。Windows Server 2003 的“路由远程访问”中提供了 NAT 功能。

8.2.4　实现参考

【实验一】 ICS 共享上网

某企业目前拥有自己独立的计算机局域网络，其接入的计算机数量为 200 余台，现向 ISP 服务商申请了一个光纤专线，以达到企业计算机局域网络访问互联网的目的，那么在现有的条件下如何实现呢？

该项目属于较为大型的项目任务，由于接入的计算机台数较多，较好的解决方案是采用专业路由器的方法，这种方案涉及专业路由器的配置技术，不在此采用，建议采用 Internet 连接共享的方法实现，其原因不仅是搭建简单，而且还能配合第三方软件的方法用于网络的日常管理。

由于采用此种方案是基于 Windows Server 2003 网络操作系统内置软件的方式实现，因此需要配置专业网络服务器，要求该服务器具备双网卡，一块网卡用于连接企业计算机局域网络；另一块网卡用于连接互联网专线，并且要求服务器安装 Windows Server 2003 网络操作系统，特别要注意在安装的过程中所允许的最大接入数量。

在本实验中，一块网卡分配有静态外部 IP 地址，通过此 IP 地址可以访问互联网；另外一块网卡分配有私有 IP 地址，接入到内部局域网中，局域网中计算机通过此网卡跟外部沟通。网络结构如图 8.4 所示。

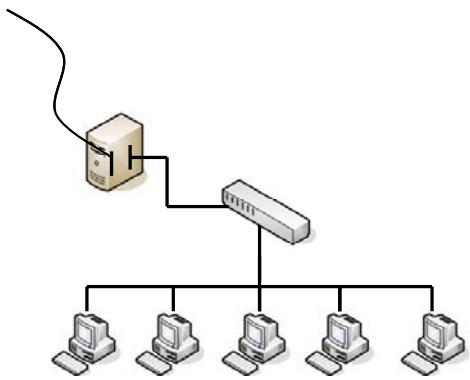

图 8.4　网络结构

【实验步骤】

（1）服务器的配置

① 打开“网络连接”，如图 8.5 所示。

图 8.5　打开网络连接

② 右键单击“外部连接”，然后单击“属性”。“外部连接“代表的是本实验中连接到外网的网卡。

③ 在“高级”选项卡的“Internet 连接共享”下，选中“允许其他网络用户通过此计算机的 Internet 连接来连接”复选框。单击“确定”按钮即可，然后退出。

（2）客户端配置

在客户机上，打开本地连接属性→单击 TCP/IP 协议属性，将本地连接的网关 DNS，都设为服务器对内网卡的 IP 地址。

【总结】

采用 Internet 连接共享的方法实现局域网共享访问互联网较为简单且易于实现，但缺乏行之有效地网络管理功能，如网络访问日志等，建议配合采用第三方的网络管理软件以实现计算机网络的日常管理功能。

【实验二】 NAT 共享上网

【实验步骤】

（1）服务器端配置

第一步，执行“开始”→“程序”→“管理工具”→“路由和远程访问”命令，打开“路由和远程访问”管理控制台。

第二步，在“路由和远程访问”管理控制台上右键击服务器图标，如图 8.6 所示。在打开的菜单中选择“配置并启用路由和远程访问”命令，进入“路由和远程访问服务器安装向导”窗口。

第三步，在打开的“路由和远程访问服务器安装向导”窗口中单击“下一步”按钮。进入图 8.7 中的“配置”窗口。在“配置”窗口中选择网络地址转换（NAT）选项，然后单击“下一步”按钮，进入图 8.8“NAT Internet 连接”窗口。

第四步，在打开的如图 8.8“NAT Internet 连接”窗口中选择需要接外网的连接，这里选择本地连接 2。单击“下一步”，进入“名称和地址转换服务”窗口，如图 8.9 所示。

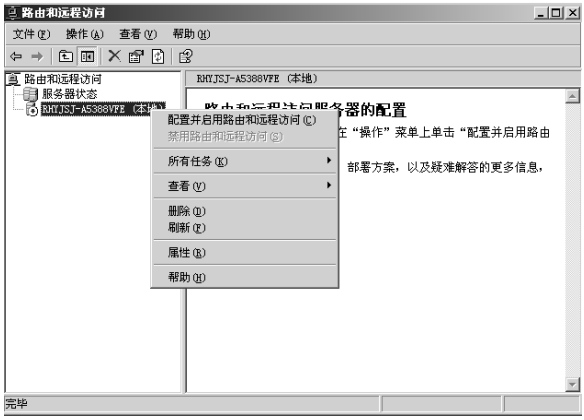

图 8.6　路由和远程访问服务器安装向导

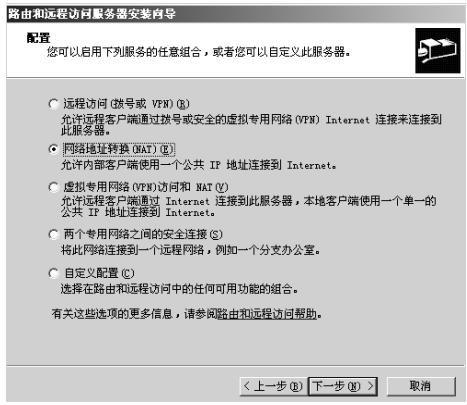

图 8.7　“路由和远程访问服务器安装向导”窗口

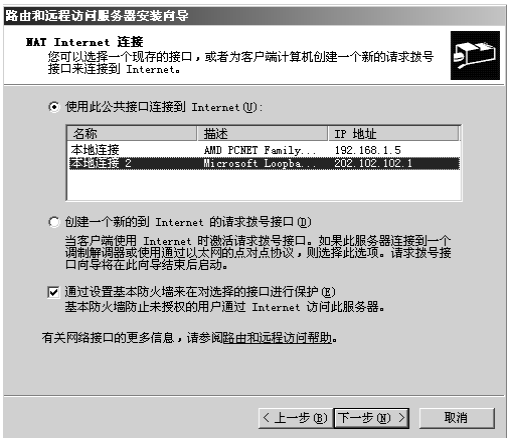

图 8.8　“NAT Internet 连接”窗口

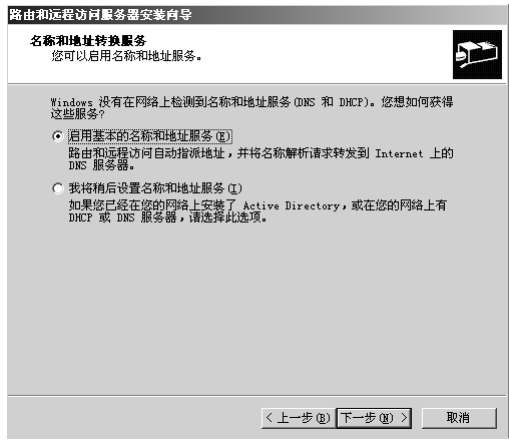

图 8.9　“名称和地址转换服务”窗口

第五步，在打开的如图 8.9“名称和地址转换服务”窗口中选择“启用基本的名称和地址服务”选项，单击“下一步”，进入“地址指派范围”窗口，然后直接单击“下一步”按钮，进入“完成”窗口，单击“完成”按钮，设置成功。

（2）客户端配置

服务端配置完成以后，还需要对客户端进行必要的配置才能正常上网。以 Windows XP 为例，在桌面上选择“网上邻居”→“属性”命令，打开“本地连接 属性”对话框。在“常规”选项卡中双击“Internet 协议（TCP/IP）”选项，在打开的“Internet 协议（TCP/IP）属性”对话框中选择“使用下面的 IP 地址”单选框。然后根据需要填写 IP 地址、子网掩码及网关。需要注意的是，这里的 IP 地址和子网掩码应该跟 NAT 服务器中的“本地连接 2”处于同一个网段，网关和 DNS 就是“本地连接 2”的 IP 地址（本例为“192.168.1.5”）。

注意：如果在局域网中配置了 DHCP 服务器，也可以选择“自动获得 IP 地址”选项。然后单击“高级”按钮，在“高级 TCP/IP 设置”对话框的“IP 设置”选项卡下单击“默认网关”区域的“添加”按钮，输入网关地址，本例为“192.168.0.5”，并单击“添加”按钮。连续单击“确定”按钮即完成配置。

项目 9

网络安全与监控管理

学习目标

在网络应用中最为常见的是如何防止计算机病毒对网络正常使用所带来的负面影响，同时也要监督和控制网络内部的活动，做到安全运行、日志记录、管理技术与措施得当。本项目通过若干任务达到如下学习目标。

- 掌握网络平台环境下软件的安装、调试与使用；
- 学会构建基于网络平台的杀毒软件的安装、配置与应用；
- 学会使用网络专业管理软件实现对网络进行监督和控制管理。

内容框架

项目 9 的内容框架如图 9.1 所示。

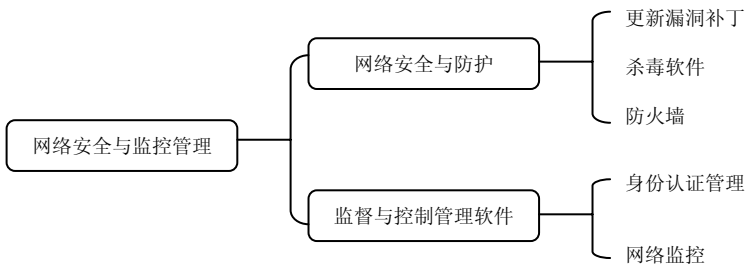

图 9.1　内容框架

任务一　网络版杀毒软件安装、配置与管理

9.1.1　任务目的

本任务的目的在于学会在计算机局域网络中安装杀毒软件网络版，并进行配置以实现客户端自动从网络服务器端进行升级，从网络管理端监控各客户端的状态，并实施相应的管理操作。

9.1.2　任务描述

将瑞星杀毒软件网络版安装在计算机局域网络中，并实现客户端的自动升级。

9.1.3　相关基础知识

单机版的杀毒软件是一个独立于计算机局域网络的个体，升级依赖于互联网连接到开发商的服务器进行更新。在计算机局域网络中如果依赖于单机版的杀毒软件，会由于各自升级先后时间的差异而造成各自版本不一致，而使计算机病毒无法从局域网中去除。网络版的杀毒软件由于升级服务器安装在局域网内部，各客户端升级速度快，版本能够很轻易地实现全网同步更新，轻松实现覆盖每台服务器和客户端的全网部署。管理员可以智能、快速、全面、直观的对全网计算机配置木马查杀、主动防御、升级等功能，实时远程获取客户端安全信息、客户端按规则自动分组管理、管理员权限分级。

瑞星杀毒软件网络版安装到服务器和客户机上后，通过“系统中心”、“服务器端”、“客户端”和“管理员控制台”4 个子系统的协同工作，实现了对网络上病毒的实时监控、定时扫描、手动扫描、自动或手动升级、信息管理等功能。同时提供了用户合法身份认证结构，保障了用户的利益，如图 9.2 所示。

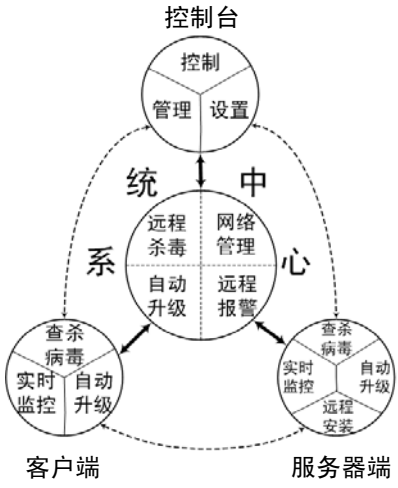

图 9.2　瑞星杀毒软件网络版工作原理

系统中心是瑞星杀毒软件网络防病毒系统命令发布、信息存储，以及安全状况分析的管理核心。它实时记录防护体系内每台计算机上的查杀病毒情况、主动防御信息、漏洞情况、安全状况等，为超级管理员分析整个网络中的安全情况提供了大量的依据。通过管理控制台发布查杀病毒、升级等各项命令，统一设置网络安全的各种策略，实现对整个防护系统的自动控制，保障整个网络安全。

注意：系统中心必须先于其他子系统安装到符合条件的服务器上，其他子系统只有在系统中心工作后，才可以实现各自的网络防护功能。

按照系统中心在局域网中的安装规模可以分为单级系统中心、多级系统中心和超级系统中心。

（1）单级系统中心：即在网络环境中仅有一个级别的系统中心，管理其客户端防病毒子系统。（说明：中小企业版属于单级系统中心产品），如图 9.3 所示。

（2）多级系统中心：在网络环境中可以安装两级系统中心，实现上级系统中心对下级系统中心及其客户端的管理（说明：企业版和企业专用版属于多级系统中心产品）。

（3）超级系统中心：在大型企业中（如跨国公司），存在着复杂的网络结构，为了提供统一的防毒管理，通过部署多层次的系统中心，将整个企业的防毒结构构建成一棵逻辑树。父系统中心可以管理其所有直属子系统中心（包括其客户端）和间接下属的系统中心（包括其客户端）；即超级系统中心可以管理到其下属的任何一级的子系统中心（包括其客户端），但是不能管理其父中心（说明：在高级企业版和高级企业专用版属于超级中心产品）。

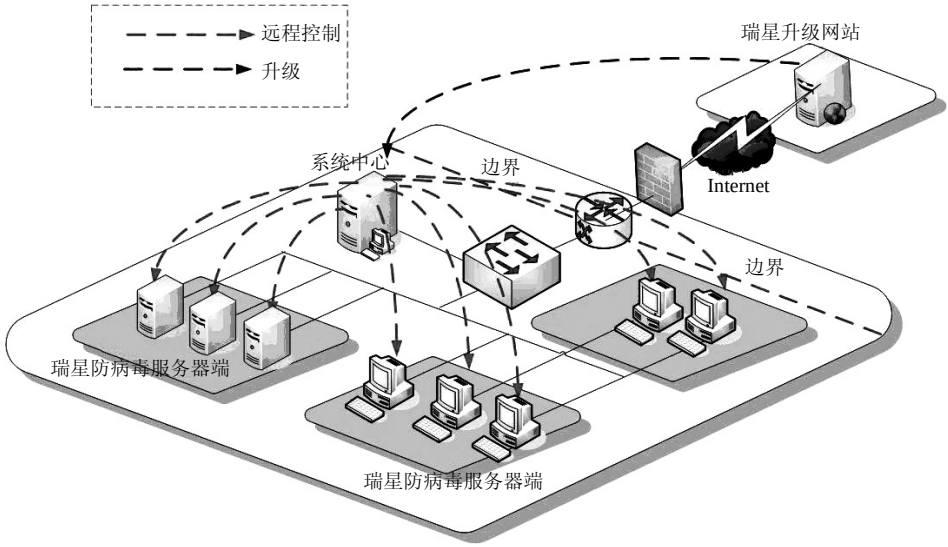

图 9.3　小型企业安装部署应用示例

9.1.4　实现参考

实验环境

剩余磁盘空间：2GB 以上，如果有漏洞扫描功能，建议将漏洞补丁保存路径所在盘保留 2GB 以上空间。

CPU：Intel Pentium IV 3.0GB 以上。

内存：1GB 以上，最大支持 4GB。

网络环境：100MB 以上网络，需要一个固定的 IP 地址。

说明：如果管理 250 台以上的客户端，建议将系统中心部署在专用服务器上。为保证防病毒系统的及时更新，请确保计算机能够实时连接 Internet。

操作系统：Windows Server 2003 企业版。

【实验一】 瑞星杀毒软件网络版安装和配置

瑞星杀毒软件网络版的基本安装对象包括“系统中心的安装”、“服务器端的安装”、“客

户端的安装”和“管理控制台的安装”。安装时先在服务器上安装“系统中心”，然后在其他计算机上安装客户端或服务器端。

【实验步骤】

（1）系统中心的安装。系统中心负责管理、协调瑞星杀毒软件网络版所有子系统的工作；实现授权许可证的验证和管理；负责瑞星杀毒软件网络版中各系统版本更新及检测和清除病毒等工作。

注意：安装系统中心时，安装程序将在该服务器上同时安装一套服务器端系统和一套管理控制台系统。

第一步，将瑞星杀毒软件网络版光盘放入光驱内，启动瑞星杀毒软件网络版安装主界面后，选择“安装系统中心组件”按钮开始安装，如图 9.4 所示。

第二步，进入安装程序欢迎界面，提示用户使用安装向导及相关建议和警告等，用户可以单击“下一步”按钮继续安装，还可以单击“取消”按钮退出安装过程，如图 9.5 所示。

图 9.4　瑞星杀毒软件网络版安装界面

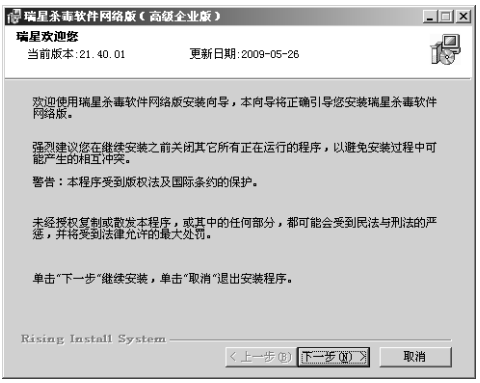

图 9.5　安装欢迎界面

注意：如果用户安装了与瑞星杀毒软件网络版冲突的软件，则会在该页面出现前弹出冲突软件提示界面。如果再继续安装本软件可能会产生问题，建议卸载后再执行本程序。

第三步，提示用户在安装前阅读“最终用户许可协议”，用户认真阅读本协议后可以选择“我接受”或“我不接受”。选择“我接受”，单击“下一步”按钮继续安装；选择“我不接受”，安装终止；单击“取消”按钮直接退出安装过程，如图 9.6 所示。

注意：选择“我接受”继续安装后，如果计算机配置了多网卡或存在多个 IP 地址将会出现“选择 IP 地址”界面。由用户指定所需 IP 作为通信 IP，为了高效通信建议采用内部网络地址。

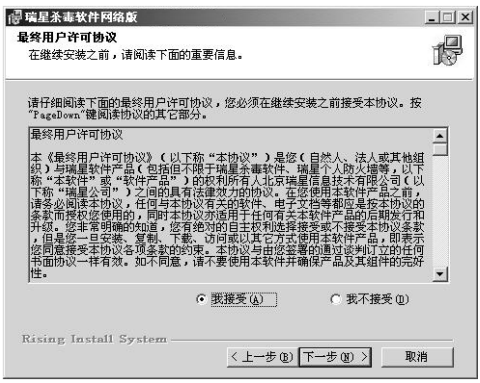

图 9.6　安装许可协议界面

第四步，根据实际需要选择相应的组件，单击“下一步”按钮继续安装，如图 9.7 所示。

第五步，进入数据库的安装界面，选择数据库的类型及相关参数。有 3 种数据库类型可

选择，分别为“在本机上安装 MSDE”、“正在运行的 MS SQL SERVER”、“已经存在的 MSDE 数据库”。默认设置为“在本机上安装 MSDE”，若网络中没有 SQL SERVER，在磁盘空间许可的情况下建议选择此项。设置 MSDE 数据库各项参数后，单击“下一步”按钮继续安装，如图 9.8 所示。

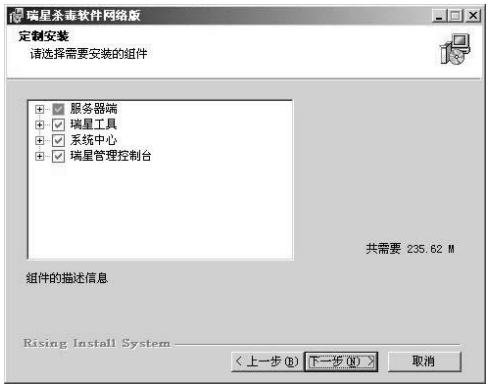

图 9.7　安装组件选择界面

图 9.8　数据库安装选择界面

若安装环境中已有 SQL SERVER，可以选择“正在运行的 MS SQL SERVER”，设置各项参数后，单击“下一步”按钮继续安装，如图 9.9 所示。

若安装环境中已有 MSDE，可以选择“已经存在的 MSDE 数据库”命令，设置各项参数后，单击“下一步”按钮继续安装，如图 9.10 所示。

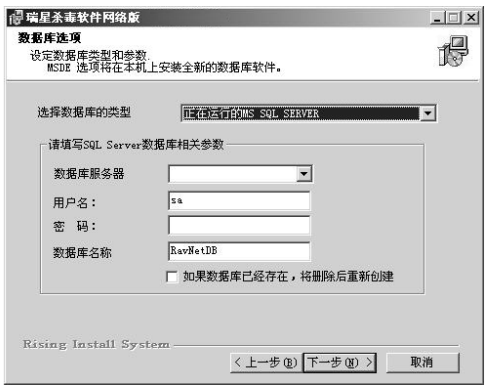

图 9.9　数据库安装选择界面

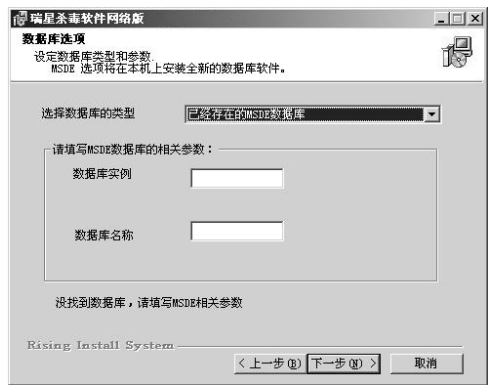

图 9.10　数据库选项安装界面

第六步，输入瑞星杀毒软件网络版产品序列号；正确输入产品序列号后，立即显示产品类型、服务器端和客户端允许安装的数量，如图 9.11 所示。

第七步，在“网络参数设置”界面显示系统中心 IP 地址，单击“下一步”按钮继续安装，如图 9.12 所示。

第八步，在“选择目标文件夹”界面中选择安装瑞星软件的目标文件夹，单击“下一步”按钮继续安装，如图 9.13 所示。

第九步，在“设置补丁包共享目录”界面中，设置提供给客户端下载补丁包的文件共享目录和共享名称，为了安装方便用户可使用默认名称，单击“下一步”按钮继续安装，如图 9.14 所示。

图 9.11 “验证产品序列号”界面

图 9.12 “网络参数设置”界面

图 9.13 “选择目标文件夹”界面

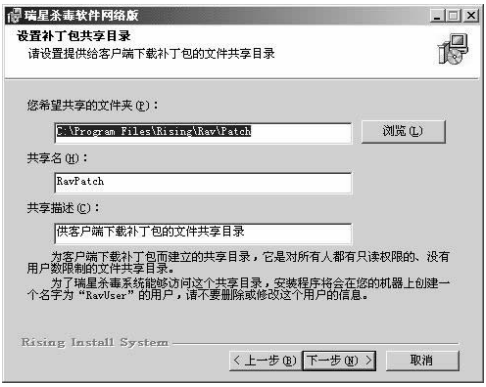

图 9.14 “设置补丁包共享目录”界面

第十步，在“瑞星杀毒系统密码”界面中，输入系统管理员密码和客户端保护密码，如不设置，默认口令都为空，在此也可以为瑞星日志查询工具中的计划任务管理预先配置向管理员发送报表的 SMTP 服务器参数，还可以单击“详细”按钮进行详细设置，设置完毕后，单击“下一步”按钮继续安装，如图 9.15 所示。

第十一步，在“选择开始菜单文件夹”界面中，输入用户需要在开始菜单文件夹中创建的程序快捷方式名称，单击“下一步”按钮继续安装，如图 9.16 所示。

图 9.15 “瑞星杀毒系统密码”界面

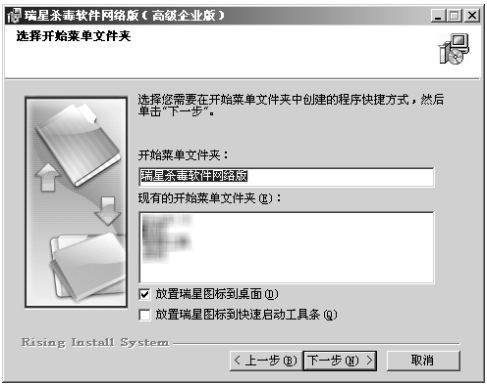

图 9.16 “选择开始菜单文件夹”界面

第十二步，在“安装准备完成”界面中确认安装信息，单击“上一步”按钮可进行修改，单击“下一步”按钮继续安装；若不勾选“安装之前执行内存病毒扫描”，将直接进入第十四步，如图 9.17 所示。

第十三步，安装程序将进行安装前的执行内存病毒扫描，单击“跳过”按钮可直接开始复制文件，建议完成系统内存病毒扫描操作后再开始复制文件，查毒完成后单击“下一步”按钮继续，安装程序将开始复制文件，如图 9.18 所示。

图 9.17 “安装准备完成”界面

图 9.18 “瑞星内存病毒扫描”界面

第十四步，显示安装过程，单击“显示信息”按钮可详细查看具体过程信息，如图 9.19 所示。

第十五步，安装结束，默认勾选“重新启动计算机”选项，单击“完成”按钮重新启动计算机完成安装。若不希望立即重新启动计算机可不勾选该选项，今后再重新启动计算机完成安装过程，如图 9.20 所示。

图 9.19 安装过程界面

图 9.20 安装完成界面

第十六步，重新启动计算机后将显示瑞星杀毒软件网络版安装过程，如图 9.21 所示。

（2）服务器端和客户端的安装。瑞星杀毒软件网络版系统中心安装完成后，就可以开始安装服务器端和客户端软件了。服务器端的安装与客户端的安装过程类似，一般可以通过本地安装、Web 安装、客户端远程安装和客户端安装包制作工具定制安装程序完成安装。

这里只介绍本地安装，其他安装方法可以参照瑞星杀毒软件网络版软件技术手册完成。为了便于服务器和客户端的安装，通常的做法是将瑞星杀毒软件网络版安装程序 Ravsetup.exe

复制到本地计算机中运行。

第一步，单击瑞星杀毒软件网络版 Ravsetup.exe 安装程序，单击“安装瑞星杀毒软件网络版服务器端”（见图 9.4）或单击“安装瑞星杀毒软件客户端”按钮，如图 9.22 所示。

图 9.21　重启安装完成界面

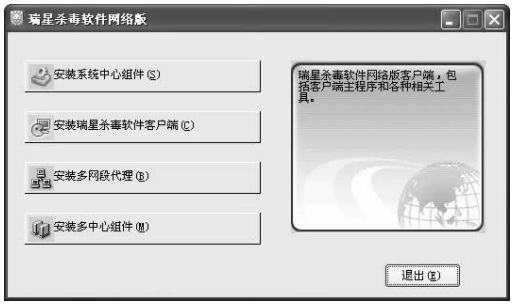

图 9.22　客户端安装界面

第二步，进入安装程序欢迎界面，单击“下一步”按钮继续安装，还可以通过“取消”按钮退出安装过程，如图 9.23 所示。

第三步，弹出“最终用户许可协议”窗口，请仔细阅读软件许可协议。如果接受该协议，选择“我接受”选项，单击“下一步”按钮继续安装；如不接受该协议，选择“我不接受”选项退出安装程序，如图 9.24 所示。

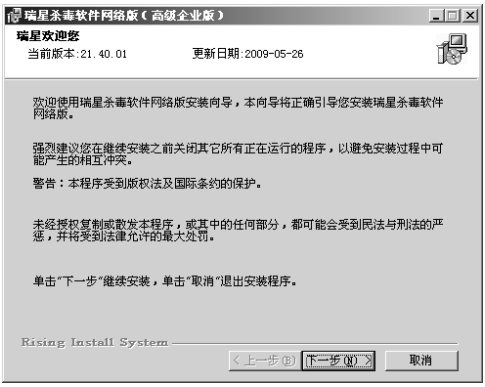

图 9.23　客户端安装欢迎界面

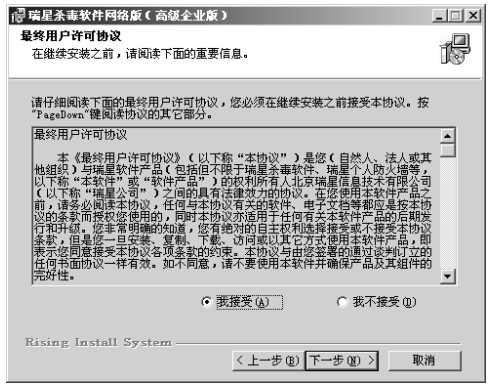

图 9.24　最终用户许可协议

第四步，进入“定制安装”界面，选择需要安装的“客户端”组件，单击“下一步”按钮继续安装，如图 9.25 所示。

第五步，进入“网络参数设置”界面，指定系统中心 IP 地址，单击“测试”按钮可以测试客户端与系统中心之间的连通性，单击“下一步”按钮继续安装，如图 9.26 所示。

第六步，在“选择目标文件夹”界面中，选择安装瑞星杀毒软件网络版的目标文件夹，单击“下一步”按钮继续安装，如图 9.27 所示。

第七步，在“选择开始菜单文件夹”界面中，输入用户需要在开始菜单文件夹中创建的程序快捷方式名称，单击“下一步”按钮继续安装，如图 9.28 所示。

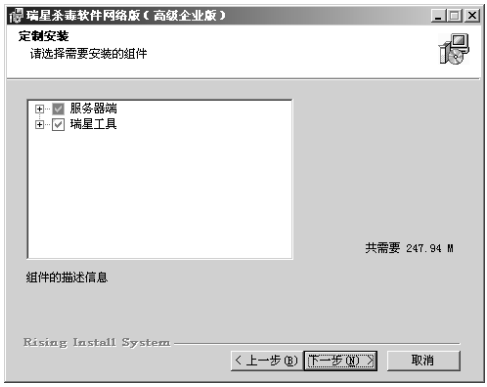

图 9.25 “定制安装”界面

图 9.26 “网络参数设置”界面

图 9.27 “选择目标文件夹”界面

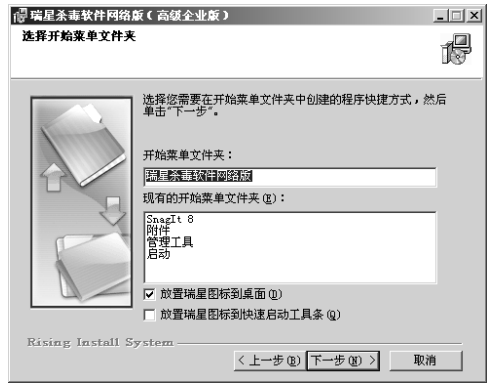

图 9.28 “选择开始菜单文件夹”界面

第八步，在“安装准备完成”界面中确认安装信息，单击“上一步”按钮可进行修改，单击“下一步”按钮继续安装；若不勾选“安装之前执行内存病毒扫描”选项，可直接进入第十步，如图 9.29 所示。

第九步，安装程序将进行安装前的系统内存查毒，单击“跳过”按钮可直接开始复制文件，建议完成系统内存查毒操作后再开始复制文件，查毒完成后单击“下一步”按钮继续，如图 9.30 所示。

图 9.29 “安装准备完成”界面

图 9.30 “瑞星内存病毒扫描”界面

第十步，文件复制结束后，单击“完成”按钮，建议用户勾选“重新启动计算机”选项则立刻重新启动计算机完成安装，若用户不勾选此项则软件不能使用，需重新启动计算机后才能正常使用，如图 9.31 所示。

图 9.31　客户端安装完成界面

（3）管理控制台的安装与使用

① 控制台的安装有通过光盘安装和控制台远程安装两种方式。

一种方式是通过光盘安装管理控制台。通过光盘安装管理控制台的操作步骤，用户可以参照系统中心的安装过程，在定制安装界面中勾选管理控制台，其他操作步骤类似。

另一种方法是远程安装管理控制台，系统管理员可以将管理控制台远程安装在其他计算机上。在计算机列表栏选中将要远程安装管理控制台的计算机，单击“操作”菜单，选择“安装管理控制台”命令，或在选中的计算机上右键单击，在弹出的菜单中选择“安装管理控制台”命令。

完成远程安装管理控制台后，在计算机列表栏中相应计算机的图标有所变化，表示该计算机已安装控制台。

注意：不要在局域网上安装过多的管理控制台，以保障管理的统一化。

② 管理控制台是在网络上集中管理所有安装有瑞星杀毒软件网络版客户端软件的计算机的管理工具。通过管理控制台可以了解整个网络中的总体安全状况并且远程管理网络中的任何一台计算机中的瑞星杀毒软件。网络上任何一台计算机的病毒警告信息都能在管理控制台得到汇总，通过管理控制台也能直观地查看网络上所有计算机当前的实时监控状态、病毒查杀情况、主动防御状态和当前版本信息等。管理控制台能对远程计算机安装瑞星杀毒软件和移动管理控制台，让管理控制台自由移动到管理员认为合适的计算机上去。管理员通过对管理控制台的操作就能对网络上所有计算机进行定期、实时地查杀病毒和全网统一升级管理，真正做到在整个网络中建立起坚实的网络病毒防护系统，如图 9.32 所示。

③ 管理控制台的启动。依次选择“开始”→“程序”→“瑞星杀毒软件”→“管理控制台”命令，或者双击桌面“管理控制台”图标，进入登录界面，如图 9.33 所示。

在“管理员登录”界面中，输入账号和口令后（默认用户名称为 admin、密码为空），单击“登录”按钮进入管理控制台界面，如图 9.33 所示。

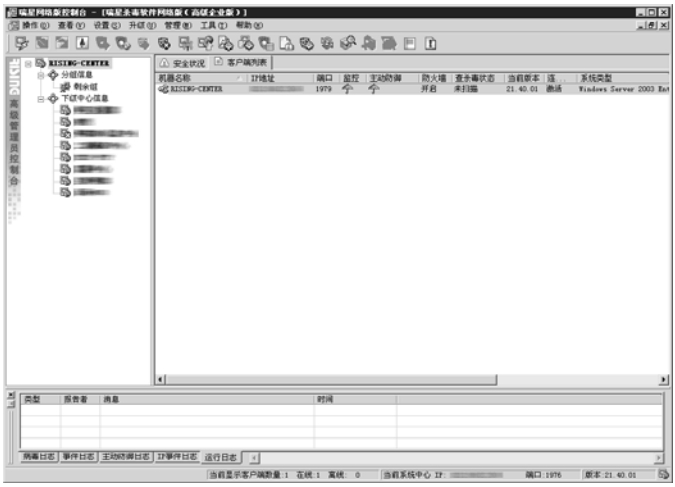

图 9.32　管理控制台

图 9.33　管理控制台管理员登录界面

④ 管理控制台界面包括 6 个部分：菜单、组管理界面、安全状况界面、客户端列表界面、日志栏界面和状态栏（参见图 9.32）。

a. 菜单包括操作、查看、设置、升级、管理、工具、帮助（如图 9.34、图 9.35 所示）。

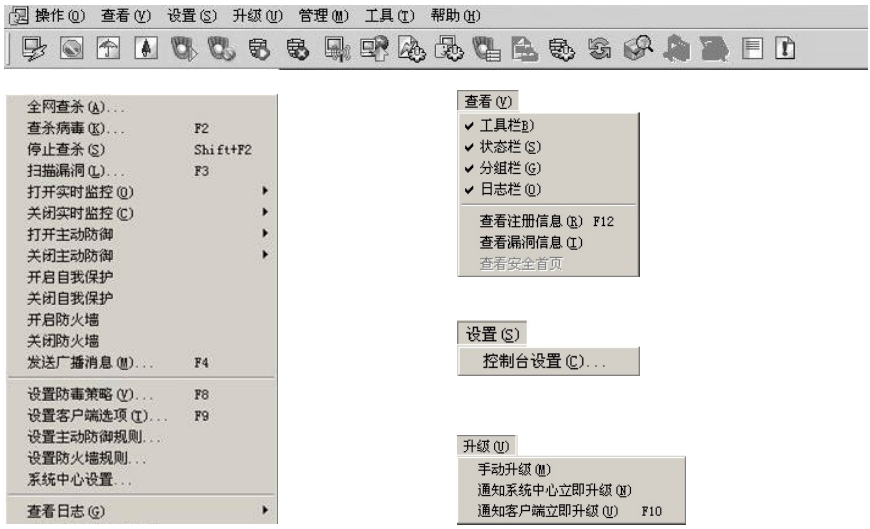

图 9.34　操作、查看、设置、升级菜单界面

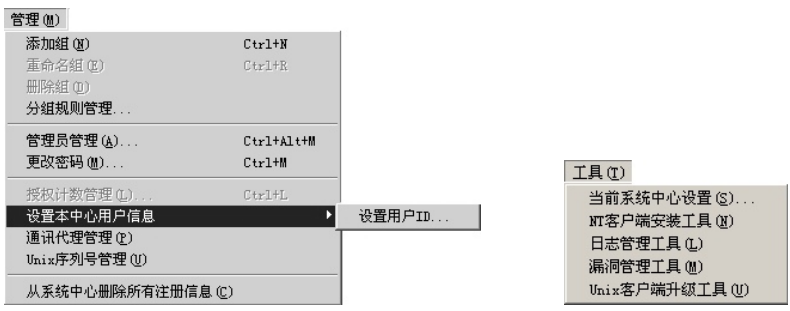

图 9.35　管理、工具菜单界面

b. 组管理界面：系统中心名称和分组信息（分组信息中默认组为“剩余组”），如图 9.36 所示。

在用户分组管理的功能界面中，能够以树形结构显示多级系统中心的层次结构。在此可以创建组、添加组成员，对各个组进行统一操作与管理。

c. 安全状况界面：显示整个网络安全情况。管理控制台通过安全状况页面显示本级中心的重要安全状况信息，使得管理员能够全面直观地了解整个网络的安全状况，其中主要内容包括：防病毒系统运行概况、重要事件和总体安全情况，如图 9.37 所示。

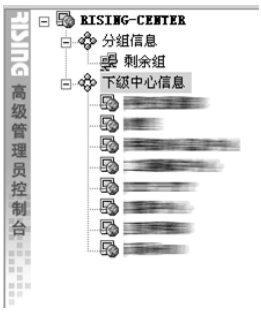

图 9.36　组管理界面

图 9.37　安全状况界面

注意：总体安全情况中显示当前系统中心内感染最多的前 5 名病毒排行和被病毒感染最多的客户端前 5 名排行情况，用户对显示的内容不能进行自定义设置。

d. 客户端列表界面：列出所有客户端及其状态。在客户端列表页面中，显示已注册到系统中心的机器名称、IP 地址、端口、监控、主动防御、防火墙、查杀毒状态、当前版本、连接以及系统类型，如图 9.38 所示。

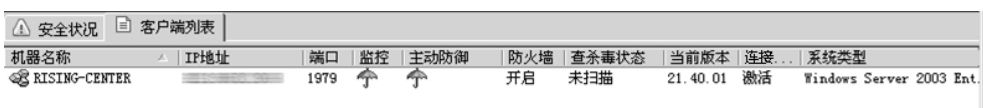

图 9.38　客户端列表界面

其中，“监控”显示监控状态，其中绿色图标代表所有监控全部开启，红色图标代表所有监控全部禁用，黄色图标代表部分监控没有开启，如果没有图标显示，则说明此客户端的监控服务未启动或未安装监控组件。

“主动防御”显示主动防御状态，其中绿色图标代表所有主动防御功能全部开启，红色图标代表所有主动防御功能全部关闭，黄色图标代表部分防御功能没有开启，如果没有图标显示，则说明此客户端的监控服务未启动或未安装主动防御组件。

e. 日志栏界面：包括病毒日志、事件日志、主动防御日志、IP 事件日志和运行日志 5 个标签页，如图 9.39 所示。它便于用户通过日志查看当前网络安全状态和安全历史记录。可以通过单击不同的标签查看指定类型的日志，默认状态显示“运行日志”。在日志信息上右键单击，可以删除所选的日志信息。

说明：其中 IP 事件日志在高级企业版中会显示；中小企业版、企业版中无此项功能。

f. 状态栏：当前显示客户端数量、当前系统中心、端口和版本。

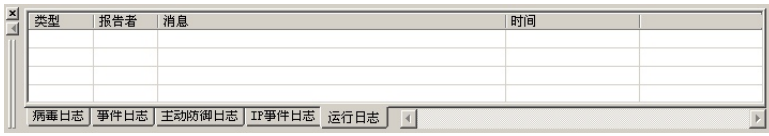

图 9.39　日志栏界面

⑤ 远程管理。远程管理功能主要是使网络管理员进行远程操作，这些操作包括为当前系统中心及其任意客户端或下级系统中心及其任意客户端进行查杀病毒、漏洞扫描、开启/关闭实时监控、开启/关闭主动防御、远程诊断客户端信息等操作。

a. 查杀病毒。在管理控制台上可以任选一台或多台计算机进行远程查杀病毒。

在计算机列表栏中选择需要查杀的计算机，右键单击，在右键菜单中选择“查杀病毒”（或单击工具栏中的 按钮，或“操作”菜单下的“查杀病毒”）后，弹出查杀选项设置界面。先在下拉列表中选择查杀路径，然后单击“开始扫描”按钮即按照默认设置开始远程查杀病毒。若需要对查杀选项进行详细设置，单击“高级选项”按钮，在出现的页面中可以设置查杀文件类型、优化选项、对查杀病毒出现的各种不同情况的处理方式、查杀优先级、报告查杀进度时间间隔等。

b. 漏洞扫描。在管理控制台上可以任选一台或多台计算机进行漏洞扫描。管理员可以通过立即执行漏洞扫描的方式，及时的了解客户端漏洞情况。

第一步，在计算机列表栏中，选中准备进行扫描的计算机，单击 按钮或选择“操作”，“扫描漏洞”，或在选定计算机上右键单击，弹出的菜单中选择“扫描漏洞”，如图 9.40 所示。

第二步，在弹出的漏洞扫描设置对话框中完成扫描设置。用户可以在“扫描系统漏洞”和“扫描不安全设置”选项前的复选框中勾选或取消勾选，扫描后会根据用户的选择显示相应的扫描信息，如图 9.41 所示。当扫描“不安全设置”时可以选择是否自动修复，勾选“自动修复不安全设置”选项将修复可以自动修复的“不安全设置”，对于不能自动修复的“不安全设置”需要用户手动修复。单击“严重级别”下拉按钮可以选择不同级别对系统漏洞和不安全设置进行扫描，分为全部、最高、中级以上、低级以上 4 种，用户可根据需求设置扫描级别。单击“开始扫描”按钮进行漏洞扫描。

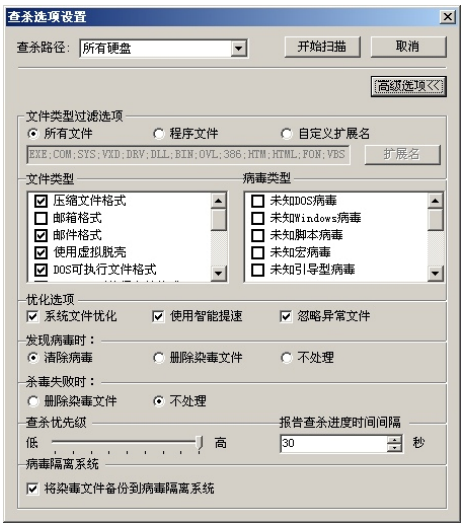

图 9.40　查杀病毒选项设置界面

图 9.41　漏洞扫描设置

注意：选择“自动修复不安全设置”选项可能会导致客户端的系统设置被修改，此项默认不勾选，请慎重操作！

第三步，在管理控制台中会显示漏洞扫描详细信息，用户可以查看结果并进行修复漏洞等操作。下面是在既选择系统漏洞又选择了不安全设置的情况下查看漏洞结果。

单击“客户端”标签，扫描结果将按客户端分类显示。选中某个计算机，在下面漏洞信息列表中选择某项漏洞信息，右键单击选择“安装补丁程序”可以通知选中计算机安装此漏洞的补丁程序；选择某项不安全设置，右键单击选择“修复不安全设置”可以为选中计算机修复此项不安全设置，如图 9.42 所示。

图 9.42　漏洞扫描扫描信息界面

在存在此漏洞的计算机列表中，选择准备安装补丁的计算机，右键单击选择“安装补丁程序”将通知所选择的计算机安装此漏洞的补丁程序。如果直接在漏洞信息上右键单击选择“安装补丁程序”，则通知列表中所有存在此漏洞的计算机安装此漏洞补丁程序。

注意：

1. 瑞星杀毒软件网络版将通过不断地升级来增加和完善漏洞信息，为保证可以扫描到最新的漏洞信息，请及时从瑞星网站更新瑞星杀毒软件网络版。

2. 由于操作系统特性不同，更新补丁后可能要求重新启动系统。

3. 瑞星杀毒软件网络版只提供补丁文件的管理和分发功能，所有补丁程序均由微软公司提供，补丁的安装过程也由微软程序完成，由于安装补丁程序或修复不安全设置引起的系统功能异常和配置修改等问题请向微软公司咨询。

4. 在扫描结果中，会出现某些补丁程序无法下载的情况，这是由于此类漏洞的修补只能利用微软公司提供的 Windows Update 来完成，微软公司并没有单独对此漏洞提供公用的补丁程序，对于此类漏洞请通过 Windows Update 功能进行更新。

c. 发送广播消息。管理员可以通过管理控制台上的广播功能对所有或指定的客户端发布文本消息。此项功能实现了管理员对客户端的文字化交流，使得管理更加周密和高效。

发送广播的步骤如下：

第一步，在计算机列表栏中选中需要接收广播的用户，单击“操作”菜单，选择“发送广播消息”，或者在选中用户的右键菜单中选择“发送广播消息”。

第二步，在弹出的“发送广播消息”对话框中输入文本信息，单击“发送”按钮，如图 9.43 所示。

第三步，目标客户端将弹出消息窗口，读取完消息后，单击“清除”按钮即可清除该消息，单击“保存”按钮，可将该广播消息保存为 *.txt 文件，如图 9.44 所示。

图 9.43 “发送广播消息”对话框

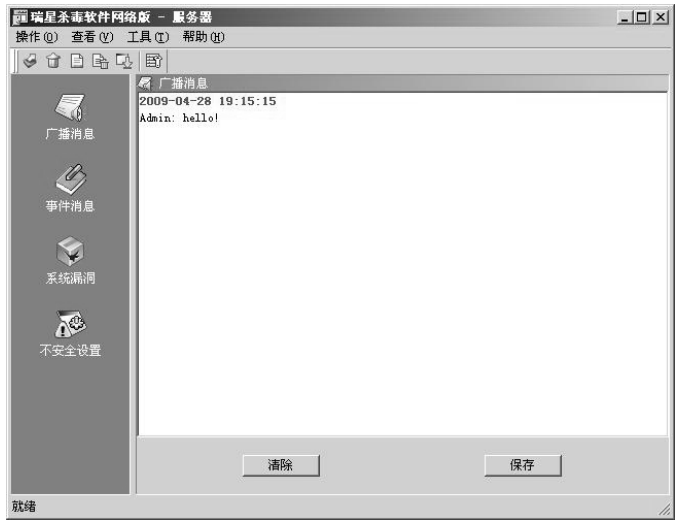

图 9.44 客户端消息界面

瑞星杀毒软件网络版是瑞星公司推出的企业级网络防病毒软件产品，它解决了以往网络防病毒软件在安装、设置、管理，以及升级时遇到的不方便与不及时等问题，全新的查杀毒技术、直观友好的操作界面、强大的 Internet 与 Intranet 防病毒能力、及时周到的技术服务，使之成为各行业推行企业防病毒解决方案的首选。这里仅介绍了其核心功能的操作，还有其他很多功能的开发使用有待于在此基础上去摸索尝试。

任务二　网络岗网络监控软件安装、配置与管理

9.2.1　任务目的

本任务的目的在于学会在计算机局域网络中安装网络监控软件，并进行配置以实现对局域网络实现全面监控与管理。

9.2.2　任务描述

将网络岗软件版安装在计算机局域网络中，并实现整个计算机局域网络的监控与管理。

9.2.3　相关基础知识

企事业单位利用内部计算机局域网络实现互联网访问，提高工作效率，加强了企业的竞争力。但是，互联网对企业内部管理的负面影响也日趋明显，在企事业单位中，分支机构多，人员架构复杂，管理要求高，必须有一套网络监控产品满足单位的网络管理需求。

“网络岗”是目前国内领先的上网监管软件，只需要通过一台计算机即可监控整个网络的网络活动，是政府机构、企事业单位和校园网吧上网的必备管理软件之一。网络岗为用户引入全新的互联网管理模式，为用户的互联网管理提供了一套详尽的方案和手段。通过网络岗对网络资源的合理配置和上网行为的策略监控，达到有效防止网络资源浪费、规范工作时间上网行为，以及防止敏感信息流失的目的，最终营造一个高效和可信赖的网络工作环境。网络岗界面直观、简单易用，适用于企业、学校、政府部门、保密单位及研究所等。

针对企事业单位计算机局域网络的差异，网络岗提供了 4 种安装方案供用户比对或选择使用，这 4 种安装方案如下。

方案 1：通过安装“代理服务器软件”或“网络岗 NAT”，实现所有机器共享上网，如图 9.45 所示。

安装方法：将“网络岗”安装在代理服务器上，绑定内网的网卡，网络岗设置为“非旁路监控”状态。常见的代理服务器软件：Microsoft ISA/Sygate/Wingate/Winroute/CCProxy/亿特代理等。

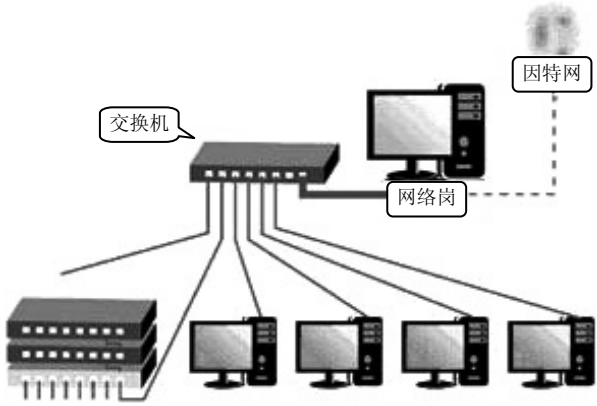

图 9.45　方案 1 安装示意图

方案 2：通过“IP 分享器、路由器或防火墙”实现整个网络共享一个出口上网，并且内部交换机均不具备设置镜像端口的功能，如图 9.46 所示。

安装方法：在内部交换机和路由器之间加一共享式 Hub，再将安装“网络岗”的机器网线也接入到 Hub 上，网络岗设置为“旁路监控”状态。

方案 3：通过“IP 分享器、路由器或防火墙”实现整个网络共享一个出口上网，且内部主交换机具备设置镜像端口的功能，如图 9.47 所示。

安装方法：在内部主交换机上设置端口镜像，将接路由器的网线设置为“被镜像端口”，将接“网络岗”的网线设置为“镜像端口”，网络岗设置为“旁路监控”状态。

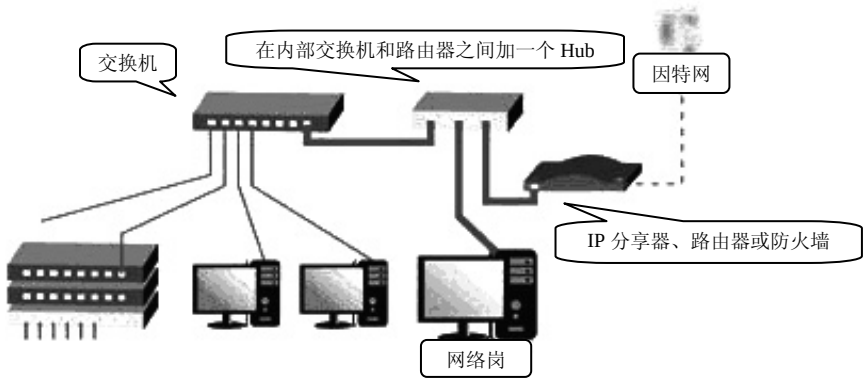

图 9.46　方案 2 安装示意图

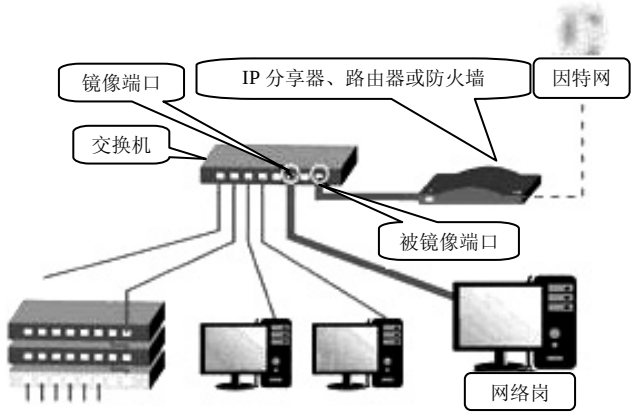

图 9.47　方案 3 安装示意图

方案 4：在一台双网卡计算机上建立“网络桥”，将该“网络桥”放在 Internet 出口处，如图 9.48 所示。

安装方法：直接将“网络岗”安装在启用“网络桥”的机器上，“网络岗”绑定靠近内网的网卡，同时给“网络桥”配置 IP 以使其能访问内部网的其他机器。网络岗设置为“非旁路监控”状态。

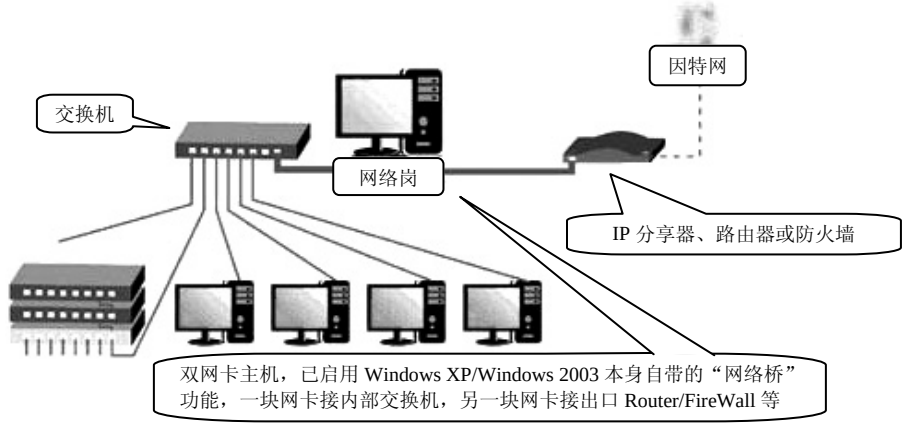

图 9.48　方案 4 安装示意图

9.2.4　实现参考

实验环境

Intel Pentium IV 1.6GBMHz 以上；剩余磁盘空间：40GB 以上；内存：512MB 以上，建议 1GB　Windows Server 2003 企业版。

【实验一】 安装和配置网络岗网络监控软件

【实验步骤】

安装网络岗网络监控软件以前，必须明确采用的安装方案、局域网络拓扑结构及安装该软件服务器所处的位置，这为以后的配置提供至关重要的信息。

网络岗第六代软件安装包共有 6 个文件，如图 9.49 所示。

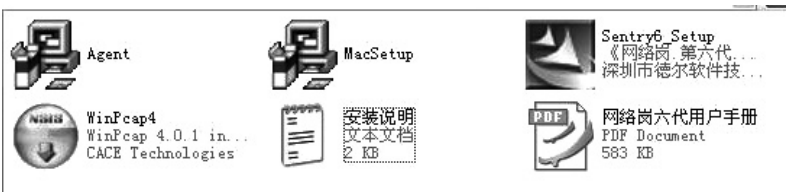

图 9.49　网络岗软件安装包

其中：

Sentry6_Setup.exe：网络岗软件安装主程序。

WinPcap4.exe：捕包驱动（以前没有安装过的计算机必须安装）。

MacSetup.exe：跨 VLAN 监控时使用，并非必须安装，安装后获取 MAC 地址更准确、及时、全面网卡地址“采集”程序，在跨 VLAN 环境且选择“基于网卡 MAC”的方式监控时才用，一般可在每个 VLAN 中安装一个，不安装也可以，安装是为了获取更及时、准确的客户机网卡地址情况，且可有效地进行 IP-MAC 绑定。

Agent.exe：内网管控程序客户端（安装在目标计算机上），用以抓屏获取系统信息等。

（1）网络岗网络监控软件安装过程

第一步，单击网络岗软件安装主程序 Sentry6_Setup.exe，如图 9.50 所示。

第二步，单击“下一步”按钮进入软件安装目录界面，选择软件安装文件夹位置，如图 9.51 所示。

图 9.50　网络岗第六代软件安装欢迎界面

图 9.51　软件安装文件夹界面

注意：由于网络岗可以实时记录网络用户的访问日志，对于用户数较多的局域网络，其访问日志文件也相对较大，因此建议将该软件安装在容量较大的存储位置。

第三步，单击“下一步”按钮后，无须单击其他选项网络岗软件即可自动安装完毕，通常最后弹出安装 WinPcap 提示，如图 9.52 所示。

第四步，单击网络岗软件安装包中的 WinPcap4.exe 捕包驱动软件，如图 9.53 所示。

注意：如果以前安装过 WinPcap 软件则可以不必再安装，但如果之前安装的版本低于 4.0，仍建议重新安装该软件。

图 9.52　提示安装 WinPcap 软件信息

图 9.53　WinPcap 软件安装界面

第五步，依次单击“下一步”按钮即可完成 WinPcap 软件的安装。

第六步，重新启动计算机后将显示瑞星杀毒软件网络版安装过程。

第七步，单击桌面“网络岗第六代”软件图标，启动网络岗软件。选择“帮助”菜单中的“产品信息”选项，单击授权信息右侧的“注册”进行产品信息注册，以获得指定的用户数和时间时效，如图 9.54 所示。

图 9.54　产品注册界面

（2）网络岗网络监控软件初始化

第一步，打开桌面“网络岗”主程序，选择捕包网卡，通常情况选一块，如图 9.55 所示。

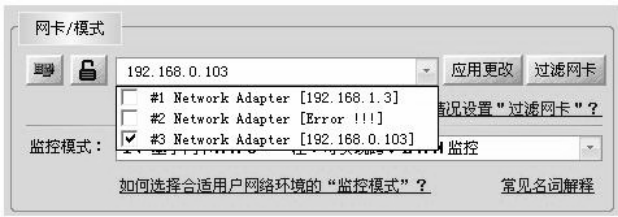

图 9.55　产品注册界面

第二步，启动网络活动监控服务，单击“全部启动”按钮，如图 9.56 所示。

第三步，搜索目标计算机，如图 9.57 所示。

图 9.56　网络活动监控启动界面

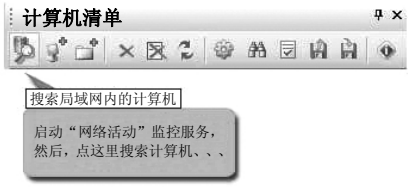

图 9.57　局域网络计算机搜索界面

如果搜索成功，会出现类似图 9.58 所示的列表。

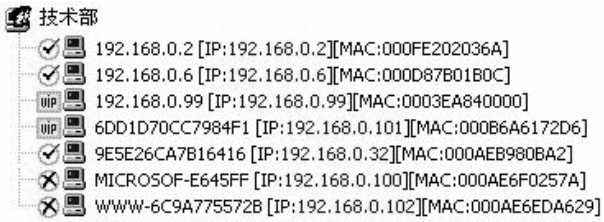

图 9.58　局域网络计算机搜索结果界面

第四步，观看效果，如图 9.59 所示。

如果网络有流量出现，则图 9.59 中的指针会摆离 0 的位置；出现摆动，说明所绑定的网卡的确有通信流量。

图 9.59　网络监控流量显示界面

（3）监控模式

①“基于网卡 MAC”的监控模式。“基于网卡 MAC”的监控就是以网卡 MAC 为依据，根据网卡 MAC 地址确定被监控的信息内容的身份。由于每台机器的网卡 MAC 相对固定，用户不容易修改，因此应该将该网络监控模式列为首选。在这种网络监控模式下，用户更换新

的网卡后，网络岗会重新检测到新的 MAC，因此，新网卡将被当做新加入的机器来处理。

注意：仅在“基于网卡 MAC”监控模式下，网络岗才具备 IP-MAC 地址绑定功能，如图 9.60 所示。

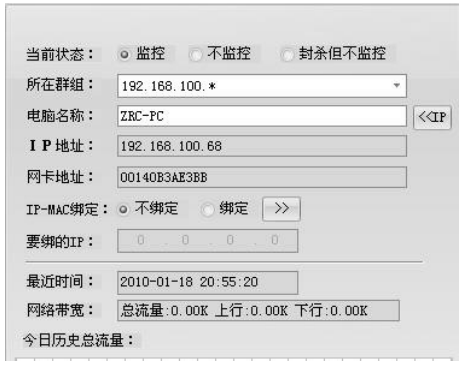

图 9.60　基于网卡 MAC 监控模式的用户初始界面

②“基于账户”监控模式。“基于账户”的监控启用后，被控用户计算机浏览网页时，弹出身份认证窗口，如图 9.61 所示。

用户必须通过身份验证才可以正常上网，这类方式特别适合酒店行业。比如，客人来后，临时分配一个密码给他，而账户名称就是其“房间编号”。“基于账户”监控时，建议用“非旁路”安装方式，如“网络桥（双网卡）”，即“一进一出”的方式；或选用“网络岗 NAT”方式。之所以建议采用这两类方式，主要是考虑到这两类方式对数据包的控制非常有效，而“旁路”的模式对 UDP 封包很困难。

③“基于 IP”监控模式。“基于 IP”的监控主要应用在大型网络，这类客户网络的特点是：网络复杂、计算机数量多、可能有多级 NAT，客户监控的目的主要是留下监控日志，并给出简单过滤规则。因为计算机数量较大，在计算机列表中如果列出所有计算机的 IP，则管理十分烦琐，所以，采用手动输入“IP 范围”作为监控目标，如图 9.62 所示。

图 9.61　用户登录界面

图 9.62　IP 搜索范围界面

归纳以上 3 种监控方式，“基于网卡 MAC”监控模式是通常情况下主要采用的一种监控方式，适合中小型网络规模的网络环境。“基于 IP”监控模式主要用于计算机数量规模大、控制要求不高的网络；基于 IP 监控时，用户可以定义 IP 范围，以简化对监控目标的管理。“基

于账户”主要针对一些特殊行业，如酒店、宾馆等。

（4）过滤规则的使用

启动网络岗后可以在“系统”菜单中选择“过滤规则”编辑过滤规则，如图 9.63 所示。

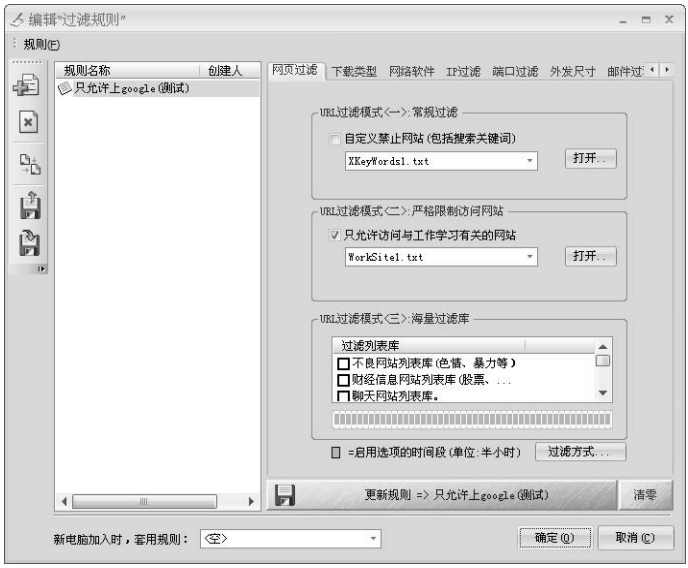

图 9.63　编辑过滤规则界面

首先单击 添加一条新规则，并命名为 Newtest，然后针对 Newtest 规则在右边选项进行规则设置，如图 9.64 所示。

①“网页过滤”规则。网页过滤主要是针对地址 URL 的过滤，对内容不予考虑；定义关键词时，建议输入最具代表性的词，如图 9.65 所示。

针对 google.com、baidu.com 和 3721 等搜索网站，还支持对中文关键词的封堵。

图 9.64　添加过滤规则界面

图 9.65　网页过滤界面

②“下载类型”。下载类型主要是根据文件的类型描述来禁止用户的过度下载，从而保证网络带宽的流畅。“禁止下载下列类型文件”中所列举的文件，通常是那些容量较大，占用网络带宽较高，会影响到整个网络流畅使用的文件，如视频文件、光盘映像文件及 BT 种子文件等。一旦选中了指定的类型文件，用户是无法下载的。除了默认的文件类型外，还可以通过单击“添加”按钮增加文件类型，如图 9.66 所示。

图 9.66　下载类型界面

③“网络软件”。在企事业单位的正常上班时间，互联网给员工提供开展业务活动的平台。为了保证工作效率，净化工作环境，就必须采取措施来禁止员工进行与工作内容无关的网络活动，如各类聊天、网上炒股、音频/视频等。“网络软件”过滤规则提供了最基本、最常见的这类网络软件的封堵手段。在所列举的网络软件列表中，可以根据实际情况来选中相关的软件名称，进而达到封堵的目的，如图 9.67 所示。

④“IP 过滤”。IP 过滤是针对互联网上各类资源的 IP 地址的过滤，进行设置时，需要对 IP 有全面的了解。可以定义某一范围内的 IP，也可以定义具体的 IP，如图 9.68 所示。

图 9.67　网络软件界面

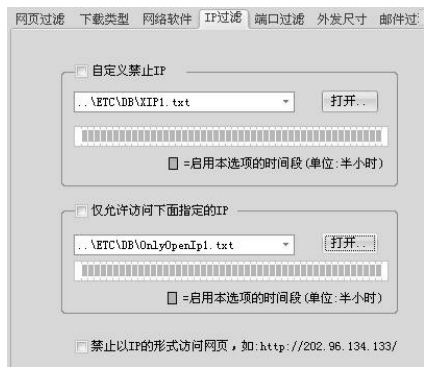

图 9.68　IP 过滤界面

⑤“端口过滤”。端口过滤即通常所说的“封堵端口”，是现有网络管理用的比较多的功能之一。

任何一款网络软件，如果它建立在 TCP/IP 通信之上，都会用到“端口”，如股票软件、FTP 软件、收发邮件软件等，都具备自己的开放端口。因此，通过“端口”来封锁上网行为是非常有效的，如图 9.69 所示。

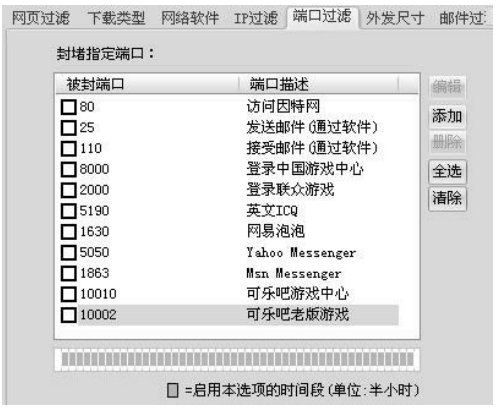

图 9.69　端口过滤界面

⑥“启用时段”与“上网时段”。“启用时段”是指当前定义的过滤规则（如 Newtest）启动的时间段，在指定启用的时间段内定义的各种过滤规则均生效，而且可以设定节假日不启用过滤规则，开放所有网络功能。图中蓝色显示块表示启用，白色表示不启用。用鼠标控制选择蓝色或白色，如图 9.70 所示。

“上网时段”只是简单地控制目标机器的上网行为，图中蓝色显示块表示允许区，白色表示禁止区。用鼠标控制选择蓝色或白色，如图 9.71 所示。

只有在白色时间段，对 Web 端口的封堵选项才起作用。在蓝色时间段是不是就一定可以上网还难说，主要看其他的项目中是否设置了封堵，在如此多的上网规则中，只要有一处封堵，就能起到封堵的作用。

图 9.70　启用时段界面

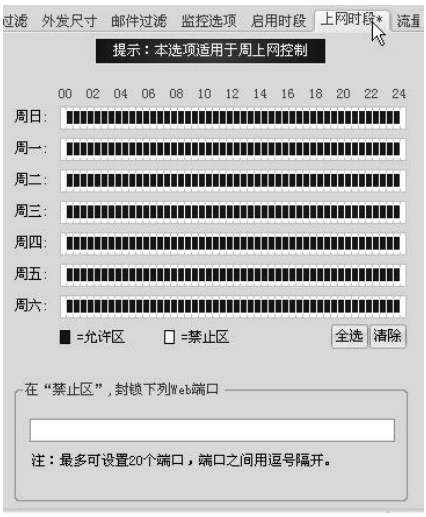

图 9.71　上网时段界面

⑦“流量限制”。对指定的用户可以限制访问流量，本规则适用于出口带宽较小的网络，用以解决网速较慢的现象。当选择限制用户的流量后，会中断用户的已有连接，如图 9.72 所示。

⑧“开放端口”。通过该过滤规则可以设定 Web 仅能访问指定的端口，进而屏蔽其他所有端口，如图 9.73 所示。

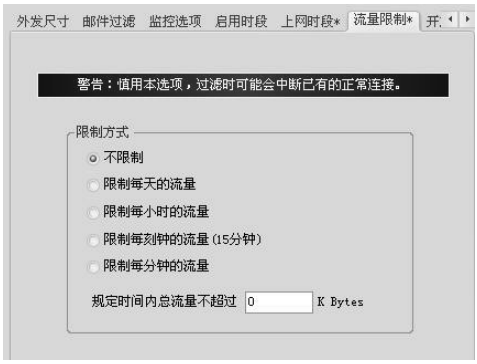

图 9.72　流量限制界面

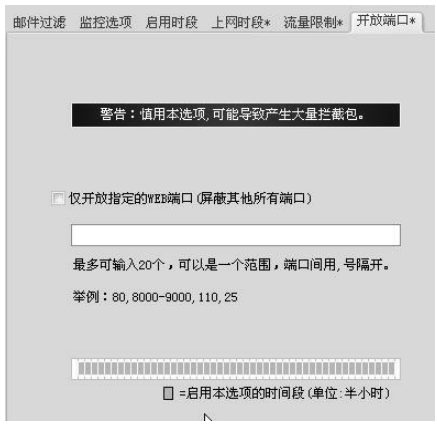

图 9.73　开放端口界面

（5）日志档案管理

①“日志档案”。网络监控重要的内容之一是网络日志档案的记载。通过“日志档案”可以设定日志存放路径及保存日志时效，如图 9.74 所示。

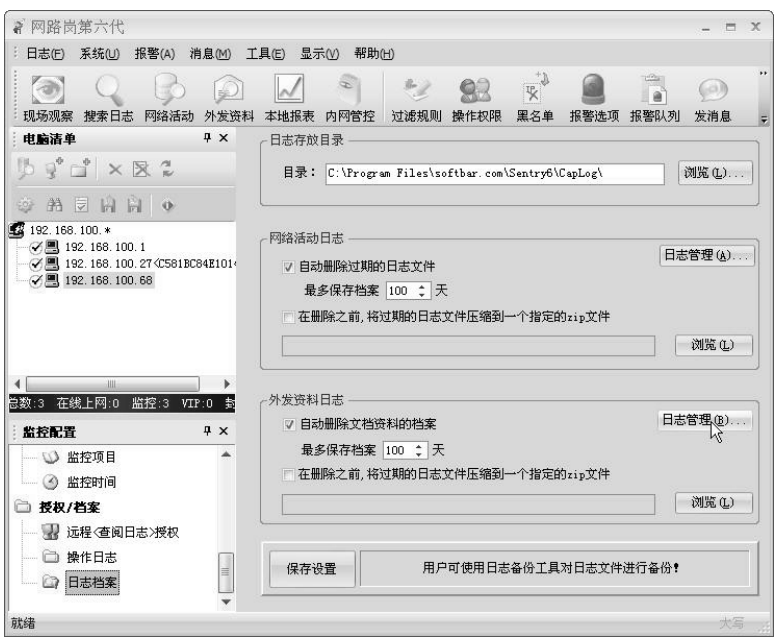

图 9.74　日志档案界面

日志存放目录：指定网络日志的存放位置，通常情况下建议指定存放在存储空间较大的位置。

网络活动日志和外发资料日志：按照我国单位互联网管理的要求，必须记载 60 天以内的上网日志，便于必要时分析、查找和定位网络使用者，因此该项最多保存档案必须大于等于 60 天，而且还可以选择将过期日志文件进行打包存放。

②“现场观察”。单击菜单“日志”选择“现场观察”或快捷按钮，可以实时观察指定用户的网络访问情况，了解和掌控用户的网络活动，如图 9.75 所示。

图 9.75　现场观察界面

③ “网络活动”。单击菜单“日志”选择“‘网络活动’日志”或快捷按钮，可以打开用户网络活动日志，浏览、分析和查找所需要的资料，如图 9.77 所示。

图 9.76　查阅网络活动日志界面

项目 10

网络高效应用

学习目标

借助于企事业单位的计算机网络平台资源，高效运行网络办公、行业网络软件，可以降低生产工作成本，提高工作效率等。本项目通过若干任务达到如下学习目标。

- 掌握网络平台环境下专用软件的安装与使用；
- 学会搭建网络即时通信平台并开展应用；
- 学会行业网络软件的安装、调试与使用。

内容框架

项目 10 的内容框架如图 10.1 所示。

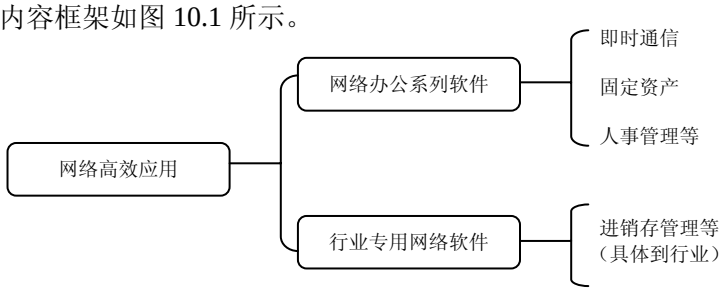

图 10.1　内容框架

任务一　企业即时通信网络平台的搭建

10.1.1　任务目的

本任务的目的是要学会在企事业单位计算机局域网络中搭建即时通信网络平台，以满足网络办公文件传送、信息传递、网络会议等最基本的需求。

10.1.2　任务描述

在企事业单位计算机局域网络中安装腾讯公司 RTX 腾讯通企业即时通信平台软件。

10.1.3　相关基础知识

在企事业单位中，畅顺的沟通对提高工作生产效率、管理质量起到至关重要的作用。在异步通信已无法满足办公需求的形式下，良好的即时沟通平台，能够帮助实现高效沟通。

腾讯通 RTX（Real Time eXchange）是腾讯公司推出的企业级即时通信平台。企业员工可以轻松地通过服务器所配置的组织架构查找需要进行通信的人员，并采用丰富的沟通方式进行实时沟通。文本消息、文件传输、直接语音会话或者视频的形式满足不同办公环境下的沟通需求。RTX 可以帮助企业员工提高工作效率，减少企业内部通信费用和出差频次。使团队和信息工作者进行更加高效的沟通。

RTX 腾讯通企业即时通信平台采用 C/S 网络架构，在服务器上需安装服务器端软件，在客户端也要安装客户端软件，如图 10.2 所示。

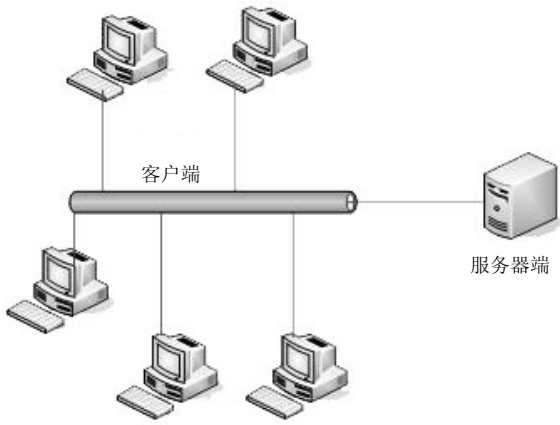

图 10.2　RTX 采用 C/S 架构

10.1.4　实现参考

实验环境

服务器端：

CPU：Intel Pentium IV 2.0GHz 以上；内存：512MB 以上；剩余磁盘空间：40GB 以上；网络环境：10MB 以上网络；操作系统：Windows Server 2000 SP4 以上。

客户端：

CPU：Intel Pentium Ⅲ 800MHzGB 以上；内存：128MB 以上；剩余磁盘空间：500MB 以上；操作系统：Windows 2000 以上。

【实验一】 搭建 RTX 腾讯通企业即时通信平台

【实验步骤】

RTX 腾讯通企业即时通信软件采用 C/S 网络架构，因此应该首先在服务器上安装服务器端软件，然后再进行客户端软件的安装。

（1）服务器端软件的安装

运行 RTX 服务器端安装软件包“rtxserver2009formal.exe”程序进行安装。安装过程中涉及“阅读许可协议”、“输入服务与许可证”、“安装路径设置”、“安装后使用者限定”等问题。如图 10.3、图 10.4 和图 10.5 所示。

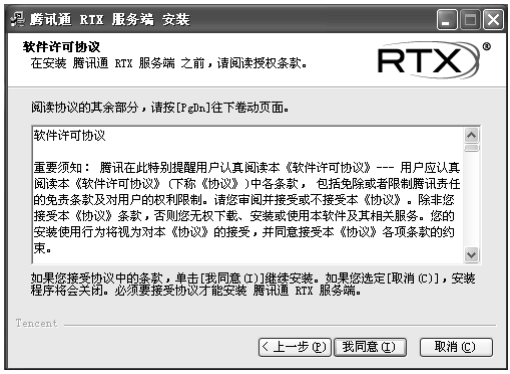

图 10.3　阅读软件许可协议

图 10.4　选择目标目录

确定了安装路径、界面语言之后，单击“安装”按钮即可完成安装。

安装完成后，将会自动打开 RTX 服务管理器进行配置，第一次安装的默认密码为空，可以通过重新设置管理员密码进行设置。

（2）客户端软件的安装

获取客户端软件安装包的方法有两种，一种是通过 Tencent 的 RTX 官方网站直接下载；另一种是通过局域网内的 RTX 服务器下载，下面介绍第二种获取客户端软件的方法。

① 首先保证服务器端软件已经安装完成。

② 启动腾讯通 RTX 管理器，界面如图 10.6 所示，红色标记内的客户端网页申请账号网址即为获取客户端软件和申请个人账号的地址。在客户端浏览器中打开此 URL 即可看到下载客户端安装包的界面，如图 10.7 所示，可快速下载客户端安装程序。

图 10.5　设置服务端界面语言

图 10.6　RTX 管理器界面

运行获取的客户端安装程序“rtxcsetup ”或网站下载的客户端安装程序“rtxclient2009formal.exe”进行安装，单击“下一步”按钮即可完成安装。安装过程遵循安装向导的提示，对“是否接受许可协议”、“个人化您的信息”、“安装路径设置”，等等，都可以采用默认设置。其中，“安装路径设置”可以由用户通过单击“浏览”按钮来选定 RTX 客户端在用户计

算机上的安装路径，具体过程不再叙述。

图 10.7　客户端安装包的界面

（3）RTX 服务器部署

服务器端安装完成后，将会自动打开管理器跳到配置向导的界面让管理器进行配置；根据配置向导配置完成，即可使用 RTX；部署主要包括管理员的配置、企业信息的配置、服务器各个进程的配置和部门用户数据的配置。

① 管理员的配置

设置管理员密码。第一次安装完成后管理员的密码默认为空，为了安全起见第一步建议先设置管理员密码；单击如图 10.8 所示的“设置超级管理员密码”即可进行设置。

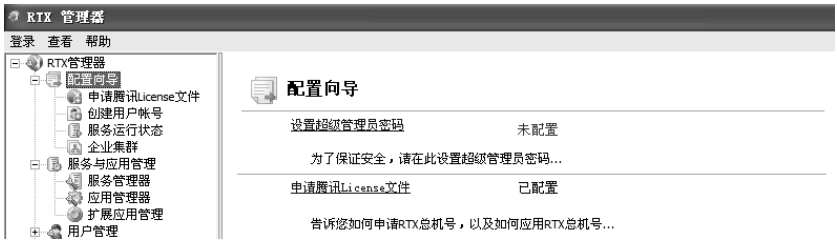

图 10.8　设置管理员密码

为了保证 RTX 管理员第一时间收到 Tencent 的版本更新或其他推广信息，配置管理员使用的 RTX 客户端账号具有管理员权限，这样其客户端面板会多一个管理员图标项。如果没有配置，每次登录管理器都会出现提醒对话框，如图 10.9 所示。

② 企业信息的配置。从腾讯网站下载的 RTX 软件是试用版，只能有 200 个客户端同时在线，正常使用 45 天并且不包含 RTX 企业总机号，不能使用 RTX 的各种插件及增值功能，如短信等。但是可以免费申请 RTX 试用 License 文件，它包含 RTX 企业总机号，可使用、购买所有 RTX 的插件及增值服务，并且可供 200 个客户端同时在线，长期使用，但需每 6 个月更新一次进行续期，续期 License 文件时请用 RTX 企业总机号访问腾讯网站 RTX 用户管理系统。

图 10.9　管理员客户端面板和提醒对话框

图 10.10　申请腾讯 License 文件

关于申请 RTX 企业总机号和 License 文件，可以单击图 10.10 中的“申请腾讯 License 文件”进行在线申请，申请成功后导入 License 文件即可。

图 10.11　申请腾讯 License 文件

③ 服务器各个进程的配置（一般情况下用默认即可）。查看并检查服务器的各个进程是否正常运行（一般情况下用默认即可）；如果运行状态不正确，可打开“服务运行状态”进行配置。在右边可以看到详细的服务信息，如需修改服务器的配置，右键单击相对的服务选择“更改配置”→“基本配置”命令，在弹出的窗口中就可以修改配置了。

（4）RTX 服务器端基本应用

① 管理部门组织结构。根据 RTX 系统的设计原则，RTX 客户端用户可以通过客户端部署界面申请 RTX 号码，也可以由系统管理人员分配 RTX 号码，然后才可以由 RTX 客户端进行登录。无论哪一种方法，都必须确定用户所属部门。因此必须首先建立企业部门组织结构。

a. 添加部门。从主界面左侧的导航栏定位“RTX 管理器”→“用户管理”→“组织架构”，然后单击“添加部门”，如图 10.12 所示。

进入添加部门的对话框之后，填写相关资料，然后单击“确定”按钮保存信息，如图 10.13 所示。

注意：设定一级部门时，“父部门”一栏一定要选定为“无”。

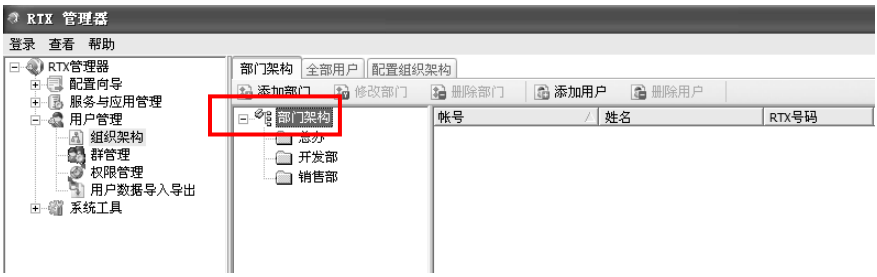

图 10.12　添加部门的弹出菜单

RTX 系统的企业部门组织结构是 RTX 用户的依附根据，因此，它的建立是以企业应用的实际需求而设定的，如图 10.14 所示，是一个企业应用中较完整的组织架构。

图 10.13　添加部门信息

图 10.14　完整的组织架构示例

b. 用户管理。RTX 管理员在按照企业实际组织结构，创建了各级部门信息之后，接下来要进行的工作，就是将企业中的每位工作人员的账号信息添加到相应的部门中，以完成企业组织的搭建。

添加 RTX 客户端用户信息有两种主要方法：一种是以向“人事部”添加用户为例，从主界面左侧的导航栏定位“RTX 服务管理”→“用户管理”→“组织架构”→“人事部”，然后右键单击弹出菜单“添加用户”，或者直接单击工具栏上的 添加用户 按钮。

另一种是进入“添加用户”对话框之后，填写资料，然后单击“添加”按钮保存信息即可完成。

注意：用户信息的“账号”、“RTX 号码”在 RTX 客户端中不能修改，如图 10.15 所示。

图 10.15　“添加用户”对话框

② 权限管理。通过主界面左侧导航栏，定位到“权限管理”项，可以看到与权限管理相关的各项内容，如图 10.16 所示。

图 10.16　导航栏中的“权限管理”

RTX 的权限分为内置权限和应用权限，内置权限是系统针对 RTX 自己功能所设置的权限；应用权限是针对所集成的插件应用功能所配置的权限，暂时还没有添加入口，如图 10.17 所示。

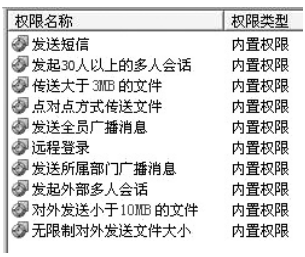

图 10.17　RTX 的内置权限

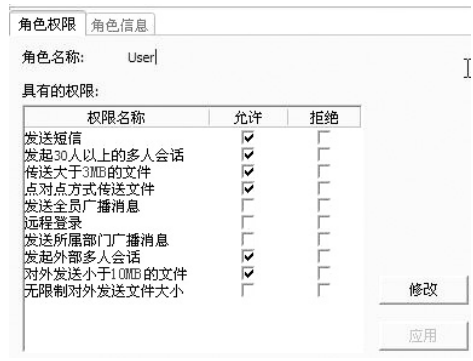

图 10.18　User 角色默认的权限

a. 内置权限。

- “发送短信”：被赋予这个权限的用户可以通过 RTX 发送手机短信。
- “发起 30 人以上的多人会话”：被赋予这个权限的用户可以发起管理员指定人数以内的多人会话，最多不超过 80 人。
- “传送大于 3MB 的文件”：被赋予这个权限的用户可以发送管理员指定大小的文件。
- “点对点方式传送文件”：被赋予这个权限的用户可以使用点对点方式传送文件。
- “发送全员广播消息”：被赋予这个权限的用户可对所在整个组织架构发送广播消息。
- “远程登录”：被赋予这个权限的用户可以使用远程登录。
- “发送所属部门广播消息”：被赋予这个权限的用户只能对所属部门发送广播消息，不能对其他部门发送广播消息。
- “发起外部多人会话”：被赋予这个权限的对外用户可以对外部企业联系人发起少于 20 人的多人会话，内部用户分配该权限不起作用。
- “对外发送小于 10MB 的文件”：被赋予这个权限的用户可以对外部企业联系人发送管理员指定大小的文件。

- “无限制对外发送文件大小”：被赋予这个权限的用户可以对外部企业联系人发送不限制大小的文件。

b. 角色。用户所具有的权限全部由角色来实现。每个角色拥有不同的权限值，让不同的用户具有不同的权限，必须通过加入角色，然后对角色分配权限来实现。系统默认一个角色 User，并默认所有用户均属于角色 User，如图 10.18 所示。

- 添加角色。单击进入权限管理页面，选择菜单栏中的“添加角色”选项，弹出“添加角色”对话框，输入角色名称和描述信息，进行角色的添加，如图 10.19 所示。

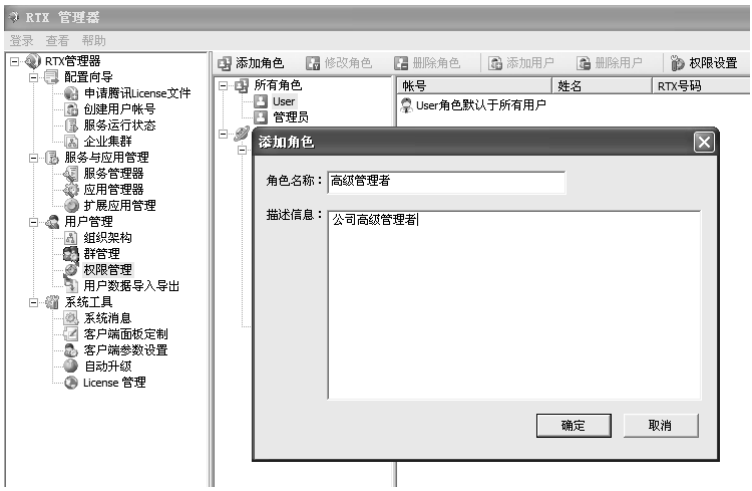

图 10.19　添加角色界面

- 为角色添加用户。选中某一角色，单击菜单栏中的“添加用户”选项，或右键单击“添加角色用户”，然后在弹出的全部用户列表中选择用户后，选择“添加”然后确定即可。这样所选择的用户就具备了该角色的权限了。

（5）RTX 客户端的基本应用

① 客户端的登录。客户端软件安装完成后，双击桌面图标或在开始菜单中选择腾讯通 RTX，将出现登录界面，用户需要在账号和密码中输入管理员分配的账号和密码，单击“登录”按钮，如果是初始登录，系统还将弹出服务器设置界面，要求输入 RTX 服务器的地址。用户需要在“服务器设置”下正确填写 RTX 服务器的网络名称或者 IP 地址，如图 10.20 所示。

图 10.20　客户端登录界面

② 客户端主界面（如图 10.21 所示）。

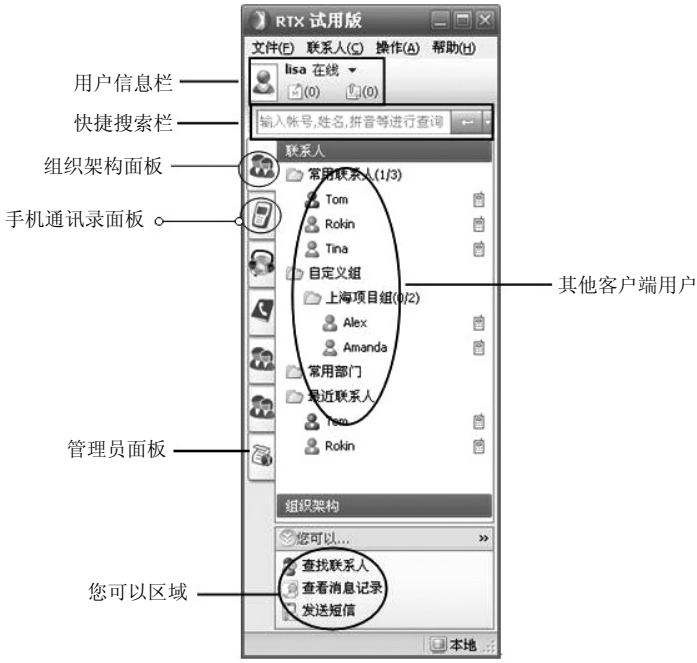

图 10.21　客户端主界面

- 用户信息栏包括用户照片、账号、状态、未读消息个数、离线消息个数几个部分。
- 快捷搜索栏主要是为了方便用户查找联系人使用，可以悬浮到桌面上的任何地方，提供账号、拼音、中文姓名的模糊查找。
- 组织架构面板由 3 个部分组成：联系人、组织架构、互联企业。
- 手机通讯录面板：在通讯录面板中，可以建立自己的外部联系人（不在本单位中）。
- 管理员面板：对于在 RTX 管理器中被设置为管理员的 RTX 用户，其主界面中将自动添加管理员页面 Tab，在该页面中可以随时关注腾讯公司的最新新闻及公告，还可以获得插件的更新信息。
- 您可以区域主要提供快捷的功能入口，比如查找联系人、查看消息记录、发送短信等常用功能。

③ 个人设置。包括基本资料、详细资料、联系方式、修改密码、热键设置、回复设置、面板设置，与腾讯 QQ 产品基本一致，不再叙述。

④ 系统设置。是对 RTX 客户端在所在机器运行时的参数设置，包括基本设置、声音设置、传输文件设置、办公集成设置等，如图 10.22 所示。

其中文件传输设置可以设置自动接收设定值以下的文件，设定值最小不能小于 1MB。还可以设置一个默认的接收传送文件的文件夹，提供清理文件目录的入口和管理目录的选项。并提供存放目录所占空间大小的检查，如果超过给定大小，RTX 将根据设定的自动清理规则进行清理。

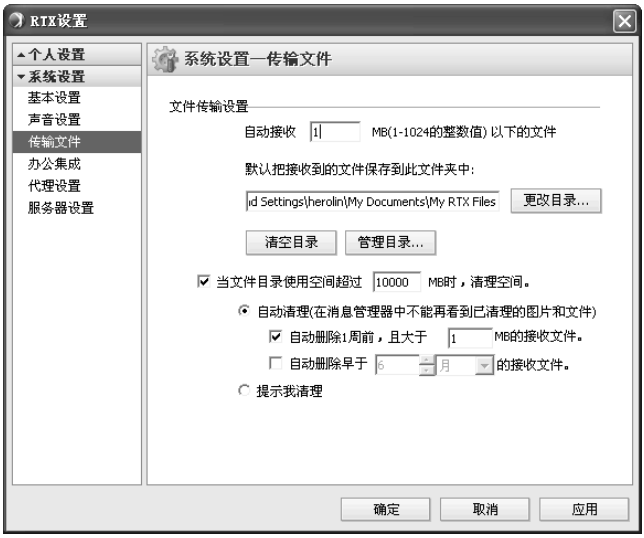

图 10.22　客户端文件传输设置

应用：

腾讯通 RTX 客户端的使用与腾讯 QQ 类似，其最大的优越性体现在文件传输速度快，可以实现离线传送信息和文件。通过服务器的合理设置，还可以用以公网登录，实现在家办公的目的。应用示例如图 10.23 所示。

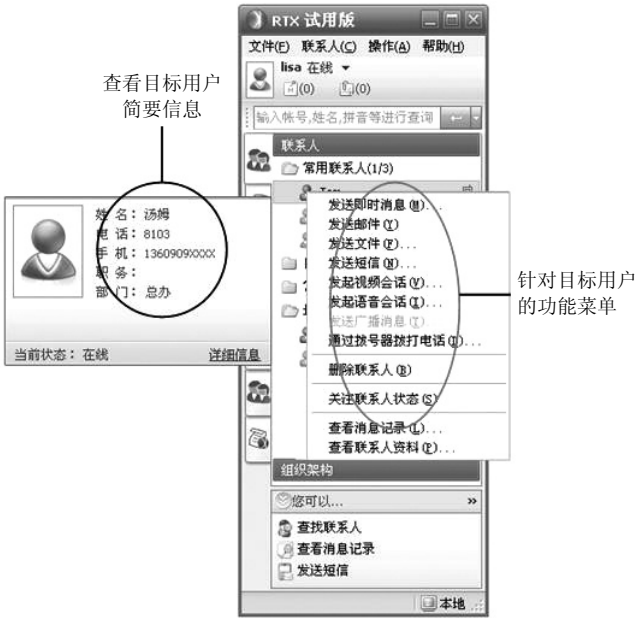

图 10.23　客户端应用功能界面